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 ٢٧ يوليو إلى ٢ أغسطس. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

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

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 27th of July to 2nd of August. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score
CVE-2025-40600	sonicwall - SonicOS	Use of Externally-Controlled Format String vulnerability in the SonicOS SSL VPN interface allows a remote unauthenticated attacker to cause service disruption.	2025-07-29	9.8
CVE-2025-31279	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.6, iPadOS 17.7.9, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to fingerprint the user.	2025-07-30	9.8
CVE-2025-43184	apple - multiple products	This issue was addressed by adding an additional prompt for user consent. This issue is fixed in macOS Sonoma 14.7.7, macOS Ventura 13.7.7, macOS Sequoia 15.4. A shortcut may be able to bypass sensitive Shortcuts app settings.	2025-07-30	9.8
CVE-2025-43186	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.6, iOS 18.6 and iPadOS 18.6, tvOS 18.6, macOS Sequoia 15.6, macOS Sonoma 14.7.7, visionOS 2.6, macOS Ventura 13.7.7. Parsing a file may lead to an unexpected app termination.	2025-07-30	9.8
CVE-2025-43189	apple - multiple products	This issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7. A malicious app may be able to read kernel memory.	2025-07-30	9.8
CVE-2025-43192	apple - multiple products	A configuration issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7. Account-driven User Enrollment may still be possible with Lockdown Mode turned on.	2025-07-30	9.8
CVE-2025-43193	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.6, macOS Ventura 13.7.7, macOS Sonoma 14.7.7. An app may be able to cause a denial-of-service.	2025-07-30	9.8
CVE-2025-43194	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to modify protected parts of the file system.	2025-07-30	9.8
CVE-2025-43198	apple - multiple products	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7. An app may be able to access protected user data.	2025-07-30	9.8
CVE-2025-43199	apple - multiple products	A permissions issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. A malicious app may be able to gain root privileges.	2025-07-30	9.8
CVE-2025-43209	apple - multiple products	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.6, iPadOS 17.7.9, iOS 18.6 and iPadOS 18.6, tvOS 18.6, macOS Sonoma 14.7.7, watchOS 11.6, visionOS 2.6, macOS Ventura 13.7.7. Processing maliciously crafted web content may lead to an unexpected Safari crash.	2025-07-30	9.8
CVE-2025-43220	apple - multiple products	This issue was addressed with improved validation of symlinks. This issue is fixed in iPadOS 17.7.9, macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to access protected user data.	2025-07-30	9.8
CVE-2025-43222	apple - multiple products	A use-after-free issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.6, iPadOS 17.7.9, macOS Ventura 13.7.7, macOS Sonoma 14.7.7. An attacker may be able to cause unexpected app termination.	2025-07-30	9.8
CVE-2025-43232	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.6, macOS Ventura 13.7.7, macOS Sonoma 14.7.7. An app may be able to bypass certain Privacy preferences.	2025-07-30	9.8
CVE-2025-43233	apple - multiple products	This issue was addressed with improved access restrictions. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. A malicious app acting as a HTTPS proxy could get access to sensitive user data.	2025-07-30	9.8

CVE-2025-43234	apple - multiple products	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in watchOS 11.6, iOS 18.6 and iPadOS 18.6, tvOS 18.6, macOS Sequoia 15.6, visionOS 2.6. Processing a maliciously crafted texture may lead to unexpected app termination.	2025-07-30	9.8
CVE-2025-43237	apple - macos	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.6. An app may be able to cause unexpected system termination.	2025-07-30	9.8
CVE-2025-43243	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.6, macOS Ventura 13.7.7, macOS Sonoma 14.7.7. An app may be able to modify protected parts of the file system.	2025-07-30	9.8
CVE-2025-43244	apple - multiple products	A race condition was addressed with improved state handling. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to cause unexpected system termination.	2025-07-30	9.8
CVE-2025-43245	apple - multiple products	A downgrade issue was addressed with additional code-signing restrictions. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to access protected user data.	2025-07-30	9.8
CVE-2025-43253	apple - multiple products	This issue was addressed with improved input validation. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7. A malicious app may be able to launch arbitrary binaries on a trusted device.	2025-07-30	9.8
CVE-2025-43261	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to break out of its sandbox.	2025-07-30	9.8
CVE-2025-43275	apple - multiple products	A race condition was addressed with additional validation. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to break out of its sandbox.	2025-07-30	9.8
CVE-2025-8454	debian - devscripts	It was discovered that uscan, a tool to scan/watch upstream sources for new releases of software, included in devscripts (a collection of scripts to make the life of a Debian Package maintainer easier), skips OpenPGP verification if the upstream source is already downloaded from a previous run even if the verification failed back then.	2025-08-01	9.8
CVE-2013-10060	netgear - DGN2200B	An authenticated OS command injection vulnerability exists in Netgear routers (tested on the DGN2200B model) firmware versions 1.0.0.36 and prior via the pppoe.cgi endpoint. A remote attacker with valid credentials can execute arbitrary commands via crafted input to the pppoe_username parameter. This flaw allows full compromise of the device and may persist across reboots unless configuration is restored.	2025-08-01	9.4
CVE-2012-10021	d-link - DIR-605L	A stack-based buffer overflow vulnerability exists in D-Link DIR-605L Wireless N300 Cloud Router firmware versions 1.12 and 1.13 via the getAuthCode() function. The flaw arises from unsafe usage of sprintf() when processing user-supplied CAPTCHA data via the FILECODE parameter in /goform/formLogin. A remote unauthenticated attacker can exploit this to execute arbitrary code with root privileges on the device.	2025-07-31	9.3
CVE-2013-10034	kaseya - KServer	An unrestricted file upload vulnerability exists in Kaseya KServer versions prior to 6.3.0.2. The uploadImage.asp endpoint allows unauthenticated users to upload files to arbitrary paths via a crafted filename parameter in a multipart/form-data POST request. Due to the lack of authentication and input sanitation, an attacker can upload a file with an .asp extension to a web-accessible directory, which can then be invoked to execute arbitrary code with the privileges of the IUSR account. The vulnerability enables remote code execution without prior authentication and was resolved in version 6.3.0.2 by removing the vulnerable uploadImage.asp endpoint.	2025-07-31	9.3
CVE-2013-10048	d-link - multiple products	An OS command injection vulnerability exists in various legacy D-Link routers—including DIR-300 rev B and DIR-600 (firmware ≤ 2.13 and ≤ 2.14b01, respectively)—due to improper input handling in the unauthenticated command.php endpoint. By sending specially crafted POST requests, a remote attacker can execute arbitrary shell commands with root privileges, allowing full takeover of the device. This includes launching services such as Telnet, exfiltrating credentials, modifying system configuration, and disrupting availability. The flaw stems from the lack of authentication and inadequate sanitation of the cmd parameter.	2025-08-01	9.3
CVE-2025-31229	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in iOS 18.6 and iPadOS 18.6. Passcode may be read aloud by VoiceOver.	2025-07-30	9.1
CVE-2025-31281	apple - multiple products	An input validation issue was addressed with improved memory handling. This issue is fixed in visionOS 2.6, tvOS 18.6, macOS Sequoia 15.6, iOS 18.6 and iPadOS 18.6. Processing a maliciously crafted file may lead to unexpected app termination.	2025-07-30	9.1
CVE-2025-43273	apple - macos	A permissions issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Sequoia 15.6. A sandboxed process may be able to circumvent sandbox restrictions.	2025-07-30	9.1
CVE-2025-31273	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in Safari 18.6, macOS Sequoia 15.6, iOS 18.6 and iPadOS 18.6, tvOS 18.6, watchOS 11.6, visionOS 2.6. Processing maliciously crafted web content may lead to memory corruption.	2025-07-30	8.8
CVE-2025-31277	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in Safari 18.6, watchOS 11.6, visionOS 2.6, iOS 18.6 and iPadOS 18.6, macOS Sequoia 15.6, tvOS 18.6. Processing maliciously crafted web content may lead to memory corruption.	2025-07-30	8.8
CVE-2025-31278	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in Safari 18.6, iPadOS 17.7.9, watchOS 11.6, visionOS 2.6, iOS 18.6 and iPadOS 18.6, macOS Sequoia 15.6, tvOS 18.6. Processing maliciously crafted web content may lead to memory corruption.	2025-07-30	8.8
CVE-2025-43270	apple - multiple products	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Sequoia 15.6, macOS Ventura 13.7.7, macOS Sonoma 14.7.7. An app may gain unauthorized access to Local Network.	2025-07-30	8.8
CVE-2025-8292	google - chrome	Use after free in Media Stream in Google Chrome prior to 138.0.7204.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2025-07-30	8.8
CVE-2025-26332	dell - TechAdvisor	TechAdvisor versions 2.6 through 3.37-30 for Dell XtremIO X2, contain(s) an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information exposure. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.	2025-07-30	8.8
CVE-2025-30105	dell - XtremIO	Dell XtremIO, version(s) 6.4.0-22, contain(s) an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information exposure. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.	2025-07-30	8.8

CVE-2013-10050	d-link - multiple products	An OS command injection vulnerability exists in multiple D-Link routers—confirmed on DIR-300 rev A (v1.05) and DIR-615 rev D (v4.13)—via the authenticated tools_vct.xgi CGI endpoint. The web interface fails to properly sanitize user-supplied input in the pingIp parameter, allowing attackers with valid credentials to inject arbitrary shell commands. Exploitation enables full device compromise, including spawning a telnet daemon and establishing a root shell. The vulnerability is present in firmware versions that expose tools_vct.xgi and use the Mathopd/1.5p6 web server. No vendor patch is available, and affected models are end-of-life.	2025-08-01	8.7
CVE-2013-10059	d-link - DIR-615H1	An authenticated OS command injection vulnerability exists in various D-Link routers (tested on DIR-615H1 running firmware version 8.04) via the tools_vct.htm endpoint. The web interface fails to sanitize input passed from the ping_ipaddr parameter to the tools_vct.htm diagnostic interface, allowing attackers to inject arbitrary shell commands using backtick encapsulation. With default credentials, an attacker can exploit this blind injection vector to execute arbitrary commands.	2025-08-01	8.6
CVE-2013-10061	netgear - DGN1000B	An authenticated OS command injection vulnerability exists in Netgear routers (tested on the DGN1000B model firmware versions 1.1.00.24 and 1.1.00.45) via the TimeToLive parameter in the setup.cgi endpoint. The vulnerability arises from improper input neutralization, enabling command injection through crafted POST requests. This flaw enables remote attackers to deploy payloads or manipulate system state post-authentication.	2025-08-01	8.6
CVE-2025-33092	ibm - multiple products	IBM Db2 for Linux 12.1.0, 12.1.1, and 12.1.2 is vulnerable to a stack-based buffer overflow in db2fm, caused by improper bounds checking. A local user could overflow the buffer and execute arbitrary code on the system.	2025-07-29	7.8
CVE-2025-24119	apple - multiple products	This issue was addressed through improved state management. This issue is fixed in macOS Sequoia 15.3, macOS Ventura 13.7.7, macOS Sonoma 14.7.7. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges.	2025-07-30	7.8
CVE-2025-31243	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.7.7, macOS Ventura 13.7.7, macOS Sequoia 15.6. An app may be able to gain root privileges.	2025-07-30	7.8
CVE-2025-31280	apple - macos	A memory corruption issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.6. Processing a maliciously crafted file may lead to heap corruption.	2025-07-30	7.8
CVE-2025-43188	apple - macos	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.6. A malicious app may be able to gain root privileges.	2025-07-30	7.8
CVE-2025-43196	apple - multiple products	A path handling issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to gain root privileges.	2025-07-30	7.8
CVE-2025-43248	apple - multiple products	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7. A malicious app may be able to gain root privileges.	2025-07-30	7.8
CVE-2025-43249	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to gain root privileges.	2025-07-30	7.8
CVE-2025-43256	apple - multiple products	This issue was addressed through improved state management. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7. An app may be able to gain root privileges.	2025-07-30	7.8
CVE-2025-43277	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 18.6 and iPadOS 18.6, watchOS 11.6, macOS Sequoia 15.6, tvOS 18.6, visionOS 2.6. Processing a maliciously crafted audio file may lead to memory corruption.	2025-07-30	7.8
CVE-2025-28170	grandstream - gxp1628_firmware	Grandstream Networks GXP1628 <=1.0.4.130 is vulnerable to Incorrect Access Control. The device is configured with directory listing enabled, allowing unauthorized access to sensitive directories and files.	2025-07-29	7.6
CVE-2024-49342	ibm - multiple products	IBM Informix Dynamic Server 12.10 and 14.10 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials.	2025-07-28	7.5
CVE-2025-24224	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in tvOS 18.5, iOS 18.5 and iPadOS 18.5, iPadOS 17.7.9, macOS Sequoia 15.5, watchOS 11.5, visionOS 2.5, macOS Ventura 13.7.7. A remote attacker may be able to cause unexpected system termination.	2025-07-30	7.5
CVE-2025-43223	apple - multiple products	A denial-of-service issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.7.7, iPadOS 17.7.9, iOS 18.6 and iPadOS 18.6, macOS Sonoma 14.7.7, watchOS 11.6, macOS Sequoia 15.6, tvOS 18.6, visionOS 2.6. A non-privileged user may be able to modify restricted network settings.	2025-07-30	7.5
CVE-2025-43227	apple - multiple products	This issue was addressed through improved state management. This issue is fixed in Safari 18.6, iOS 18.6 and iPadOS 18.6, macOS Sequoia 15.6, tvOS 18.6, watchOS 11.6, visionOS 2.6. Processing maliciously crafted web content may disclose sensitive user information.	2025-07-30	7.5
CVE-2025-24853	apache - jspwiki	A carefully crafted request when creating a header link using the wiki markup syntax, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. Further research by the JSPWiki team showed that the markdown parser allowed this kind of attack too. Apache JSPWiki users should upgrade to 2.12.3 or later.	2025-07-31	7.5
CVE-2025-2824	ibm - Operational Decision Manager	IBM Operational Decision Manager 8.11.0.1, 8.11.1.0, 8.12.0.1, 9.0.0.1, and 9.5.0 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim.	2025-08-01	7.4
CVE-2025-36611	dell - multiple products	Dell Encryption and Dell Security Management Server, versions prior to 11.11.0, contain an Improper Link Resolution Before File Access ('Link Following') Vulnerability. A local malicious user could potentially exploit this vulnerability, leading to privilege escalation.	2025-07-30	7.3
CVE-2025-43221	apple - multiple products	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.6, iOS 18.6 and iPadOS 18.6, visionOS 2.6, tvOS 18.6. Processing a maliciously crafted media file may lead to unexpected app termination or corrupt process memory.	2025-07-30	7.1

CVE-2025-43224	apple - multiple products	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in visionOS 2.6, tvOS 18.6, macOS Sequoia 15.6, iOS 18.6 and iPadOS 18.6. Processing a maliciously crafted media file may lead to unexpected app termination or corrupt process memory.	2025-07-30	7.1
CVE-2025-43239	apple - multiple products	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. Processing a maliciously crafted file may lead to unexpected app termination.	2025-07-30	7.1
CVE-2025-43254	apple - multiple products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Sequoia 15.6, macOS Ventura 13.7.7, macOS Sonoma 14.7.7. Processing a maliciously crafted file may lead to unexpected app termination.	2025-07-30	7.1
CVE-2025-53711	tp-link - tl-wr841n_firmware	A vulnerability has been found in TP-Link TL-WR841N V11. The vulnerability exists in the /userRpm/WlanNetworkRpm.htm file due to missing input parameter validation, which may lead to the buffer overflow to cause a crash of the web service and result in a denial-of-service (DoS) condition. The attack may be launched remotely. This vulnerability only affects products that are no longer supported by the maintainer.	2025-07-29	6.9
CVE-2025-53712	tp-link - tl-wr841n_firmware	A vulnerability has been found in TP-Link TL-WR841N V11. The vulnerability exists in the /userRpm/WlanNetworkRpm_AP.htm file due to missing input parameter validation, which may lead to the buffer overflow to cause a crash of the web service and result in a denial-of-service (DoS) condition. The attack may be launched remotely. This vulnerability only affects products that are no longer supported by the maintainer.	2025-07-29	6.9
CVE-2025-53713	tp-link - tl-wr841n_firmware	A vulnerability has been found in TP-Link TL-WR841N V11. The vulnerability exists in the /userRpm/WlanNetworkRpm_APC.htm file due to missing input parameter validation, which may lead to the buffer overflow to cause a crash of the web service and result in a denial-of-service (DoS) condition. The attack may be launched remotely. This vulnerability only affects products that are no longer supported by the maintainer.	2025-07-29	6.9
CVE-2025-53714	tp-link - tl-wr841n_firmware	A vulnerability has been found in TP-Link TL-WR841N V11. The vulnerability exists in the /userRpm/WzdWlanSiteSurveyRpm_AP.htm file due to missing input parameter validation, which may lead to the buffer overflow to cause a crash of the web service and result in a denial-of-service (DoS) condition. The attack may be launched remotely. This vulnerability only affects products that are no longer supported by the maintainer.	2025-07-29	6.9
CVE-2025-53715	tp-link - tl-wr841n_firmware	A vulnerability has been found in TP-Link TL-WR841N V11. The vulnerability exists in the /userRpm/Wan6to4TunnelCfgRpm.htm file due to missing input parameter validation, which may lead to the buffer overflow to cause a crash of the web service and result in a denial-of-service (DoS) condition. The attack may be launched remotely. This vulnerability only affects products that are no longer supported by the maintainer.	2025-07-29	6.9
CVE-2013-10063	netgear - SPH200D	A path traversal vulnerability exists in the Netgear SPH200D Skype phone firmware versions <= 1.0.4.80 in its embedded web server. Authenticated attackers can exploit crafted GET requests to access arbitrary files outside the web root by injecting traversal sequences. This can expose sensitive system files and configuration data.	2025-08-01	6.9
CVE-2025-28172	grandstream - ucm6510_firmware	Grandstream Networks UCM6510 v1.0.20.52 and before is vulnerable to Improper Restriction of Excessive Authentication Attempts. An attacker can perform an arbitrary number of authentication attempts using different passwords and eventually gain access to the targeted account using a brute force attack.	2025-07-29	6.5
CVE-2025-28171	grandstream - ucm6510_firmware	An issue in Grandstream UCM6510 v.1.0.20.52 and before allows a remote attacker to obtain sensitive information via the Login function at /cgi and /webrtccgi.	2025-07-29	6.5
CVE-2025-36010	ibm - multiple products	IBM Db2 for Linux 12.1.0, 12.1.1, and 12.1.2 could allow an unauthenticated user to cause a denial of service due to executable segments that are waiting for each other to release a necessary lock.	2025-07-29	6.5
CVE-2024-49828	ibm - Db2	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5.0.0 through 10.5.0.11, 11.1.0 through 11.1.4.7, 11.5.0 through 11.5.9, and 12.1.0 through 12.1.2 is vulnerable to a denial of service as the server may crash under certain conditions with a specially crafted query.	2025-07-29	6.5
CVE-2024-51473	ibm - Db2	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5.0.0 through 10.5.0.11, 11.1.0 through 11.1.4.7, 11.5.0 through 11.5.9, and 12.1.0 through 12.1.2 is vulnerable to a denial of service as the server may crash under certain conditions with a specially crafted query.	2025-07-29	6.5
CVE-2025-36071	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.5.0 through 11.5.9 and 12.1.0 through 12.1.2 is vulnerable to a denial of service as the server may crash under certain conditions with a specially crafted query due to improper release of memory resources.	2025-07-29	6.5
CVE-2025-24188	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in Safari 18.6, macOS Sequoia 15.6. Processing maliciously crafted web content may lead to an unexpected Safari crash.	2025-07-30	6.5
CVE-2025-43212	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in Safari 18.6, macOS Sequoia 15.6, iOS 18.6 and iPadOS 18.6, tvOS 18.6, watchOS 11.6, visionOS 2.6. Processing maliciously crafted web content may lead to an unexpected Safari crash.	2025-07-30	6.5
CVE-2025-43213	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in Safari 18.6, macOS Sequoia 15.6, iOS 18.6 and iPadOS 18.6, tvOS 18.6, watchOS 11.6, visionOS 2.6. Processing maliciously crafted web content may lead to an unexpected Safari crash.	2025-07-30	6.5
CVE-2025-43214	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in Safari 18.6, watchOS 11.6, iOS 18.6 and iPadOS 18.6, tvOS 18.6, macOS Sequoia 15.6, visionOS 2.6. Processing maliciously crafted web content may lead to an unexpected Safari crash.	2025-07-30	6.5
CVE-2025-43216	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in Safari 18.6, watchOS 11.6, iOS 18.6 and iPadOS 18.6, iPadOS 17.7.9, tvOS 18.6, macOS Sequoia 15.6, visionOS 2.6. Processing maliciously crafted web content may lead to an unexpected Safari crash.	2025-07-30	6.5
CVE-2025-43252	apple - macos	This issue was addressed by adding an additional prompt for user consent. This issue is fixed in macOS Sequoia 15.6. A website may be able to access sensitive user data when resolving symlinks.	2025-07-30	6.5
CVE-2025-54656	apache - struts_extras	** UNSUPPORTED WHEN ASSIGNED ** Improper Output Neutralization for Logs vulnerability in Apache Struts.	2025-07-30	6.5

		This issue affects Apache Struts Extras: before 2. When using LookupDispatchAction, in some cases, Struts may print untrusted input to the logs without any filtering. Specially-crafted input may lead to log output where part of the message masquerades as a separate log line, confusing consumers of the logs (either human or automated). 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.		
CVE-2025-30480	dell - PowerProtect Data Manager	Dell PowerProtect Data Manager, versions prior to 19.19, contain(s) an Improper Input Validation vulnerability in PowerProtect Data Manager. A low privileged attacker with remote access could potentially exploit this vulnerability to read arbitrary files.	2025-07-30	6.5
CVE-2025-36608	dell - smartfabric_os10	Dell SmartFabric OS10 Software, versions prior to 10.6.0.5, contains an Improper Restriction of XML External Entity Reference vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Unauthorized access.	2025-07-30	6.5
CVE-2025-36039	ibm - aspera_faspex	IBM Aspera Faspex 5.0.0 through 5.0.12.1 could allow an authenticated user to perform unauthorized actions due to client-side enforcement of sever side security mechanisms,	2025-07-31	6.5
CVE-2025-36040	ibm - aspera_faspex	IBM Aspera Faspex 5.0.0 through 5.0.12.1 could allow an authenticated user to perform unauthorized actions due to client-side enforcement of sever side security mechanisms.	2025-07-31	6.5
CVE-2025-33118	ibm - QRadar SIEM	IBM QRadar SIEM 7.5 through 7.5.0 Update Pack 12 is vulnerable to stored cross-site scripting. This vulnerability allows authenticated users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-08-01	6.4
CVE-2025-31275	apple - macos	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.6. A sandboxed process may be able to launch any installed app.	2025-07-30	6.2
CVE-2025-43191	apple - multiple products	A path handling issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to cause a denial-of-service.	2025-07-30	6.2
CVE-2025-43211	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in Safari 18.6, macOS Sequoia 15.6, iPadOS 17.7.9, iOS 18.6 and iPadOS 18.6, tvOS 18.6, watchOS 11.6, visionOS 2.6. Processing web content may lead to a denial-of-service.	2025-07-30	6.2
CVE-2025-43240	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.6, Safari 18. 6. A download's origin may be incorrectly associated.	2025-07-30	6.2
CVE-2025-43229	apple - multiple products	This issue was addressed through improved state management. This issue is fixed in macOS Sequoia 15.6, Safari 18. 6. Processing maliciously crafted web content may lead to universal cross site scripting.	2025-07-30	6.1
CVE-2024-45515	zimbra - collaboration	An issue was discovered in Zimbra Collaboration (ZCS) through 10.1. A Cross-Site Scripting (XSS) vulnerability exists in Zimbra webmail due to insufficient validation of the content type metadata when importing files into the briefcase. Attackers can exploit this issue by crafting a file with manipulated metadata, allowing them to bypass content type checks and execute arbitrary JavaScript within the victim's session.	2025-07-30	6.1
CVE-2025-24854	apache - jspwiki	A carefully crafted request using the Image plugin could trigger an XSS vulnerability on Apache JSPWiki, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. Apache JSPWiki users should upgrade to 2.12.3 or later.	2025-07-31	6.1
CVE-2025-43185	apple - macos	A downgrade issue was addressed with additional code-signing restrictions. This issue is fixed in macOS Sequoia 15.6. An app may be able to access protected user data.	2025-07-30	5.5
CVE-2025-43195	apple - multiple products	An issue existed in the handling of environment variables. This issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to access sensitive user data.	2025-07-30	5.5
CVE-2025-43215	apple - macos	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.6. Processing a maliciously crafted image may result in disclosure of process memory.	2025-07-30	5.5
CVE-2025-43218	apple - macos	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Sequoia 15.6. Processing a maliciously crafted USD file may disclose memory contents.	2025-07-30	5.5
CVE-2025-43225	apple - multiple products	A logging issue was addressed with improved data redaction. This issue is fixed in macOS Sequoia 15.6, iPadOS 17.7.9, macOS Ventura 13.7.7, macOS Sonoma 14.7.7. An app may be able to access sensitive user data.	2025-07-30	5.5
CVE-2025-43235	apple - macos	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.6. An app may be able to cause a denial-of-service.	2025-07-30	5.5
CVE-2025-43241	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.6, macOS Ventura 13.7.7, macOS Sonoma 14.7.7. An app may be able to read files outside of its sandbox.	2025-07-30	5.5
CVE-2025-43246	apple - multiple products	This issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7. An app may be able to access sensitive user data.	2025-07-30	5.5
CVE-2025-43247	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. A malicious app with root privileges may be able to modify the contents of system files.	2025-07-30	5.5
CVE-2025-43251	apple - macos	An authorization issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15.6. A local attacker may gain access to Keychain items.	2025-07-30	5.5
CVE-2025-43267	apple - macos	An injection issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.6. An app may be able to access sensitive user data.	2025-07-30	5.5

CVE-2025-30103	dell - smartfabric_os10	Dell SmartFabric OS10 Software, versions prior to 10.6.0.5 contains a Files or Directories Accessible to External Parties vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Filesystem access for attacker.	2025-07-30	5.5
CVE-2024-49343	ibm - multiple products	IBM Informix Dynamic Server 12.10 and 14.10 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site.	2025-07-28	5.4
CVE-2025-47001	adobe - multiple products	Adobe Experience Manager versions 6.5.22 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.	2025-07-30	5.4
CVE-2025-26400	solarwinds - Web Help Desk	SolarWinds Web Help Desk was reported to be affected by an XML External Entity Injection (XXE) vulnerability that could lead to information disclosure. A valid, low-privilege access is required unless the attacker had access to the local server to modify configuration files.	2025-07-29	5.3
CVE-2025-2533	ibm - multiple products	IBM Db2 for Linux 12.1.0, 12.1.1, and 12.1.2 is vulnerable to a denial of service as the server may crash under certain conditions with a specially crafted query.	2025-07-29	5.3
CVE-2025-33114	ibm - multiple products	IBM Db2 for Linux 12.1.0, 12.1.1, and 12.1.2 is vulnerable to denial of service with a specially crafted query under certain non-default conditions.	2025-07-29	5.3
CVE-2025-31276	apple - multiple products	This issue was addressed through improved state management. This issue is fixed in iOS 18.6 and iPadOS 18.6, iPadOS 17.7.9. Remote content may be loaded even when the 'Load Remote Images' setting is turned off.	2025-07-30	5.3
CVE-2025-43276	apple - macos	A logic error was addressed with improved error handling. This issue is fixed in macOS Sequoia 15.6. iCloud Private Relay may not activate when more than one user is logged in at the same time.	2025-07-30	5.3
CVE-2025-43260	apple - multiple products	This issue was addressed with improved data protection. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7. An app may be able to hijack entitlements granted to other privileged apps.	2025-07-30	5.1
CVE-2025-43266	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to break out of its sandbox.	2025-07-30	5.1
CVE-2024-52894	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5.0.0 through 10.5.0.11, 11.1.0 through 11.1.4.7, 11.5.0 through 11.5.9, and 12.1.0 through 12.1.2 is vulnerable to a denial of service as the server may crash under certain conditions with a specially crafted query.	2025-07-29	4.9
CVE-2025-8224	gnu - binutils	A vulnerability has been found in GNU Binutils 2.44 and classified as problematic. This vulnerability affects the function bfd_elf_get_str_section of the file bfd/elf.c of the component BFD Library. The manipulation leads to null pointer dereference. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The name of the patch is db856d41004301b3a56438efd957ef5cabb91530. It is recommended to apply a patch to fix this issue.	2025-07-27	4.8
CVE-2025-8225	gnu - binutils	A vulnerability was found in GNU Binutils 2.44 and classified as problematic. This issue affects the function process_debug_info of the file binutils/dwarf.c of the component DWARF Section Handler. The manipulation leads to memory leak. Attacking locally is a requirement. The identifier of the patch is e51fdff7d2e538c0e5accdd65649ac68e6e0ddd4. It is recommended to apply a patch to fix this issue.	2025-07-27	4.8
CVE-2025-43259	apple - multiple products	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An attacker with physical access to a locked device may be able to view sensitive user information.	2025-07-30	4.6
CVE-2025-41241	vmware - multiple products	VMware vCenter contains a denial-of-service vulnerability. A malicious actor who is authenticated through vCenter and has permission to perform API calls for guest OS customisation may trigger this vulnerability to create a denial-of-service condition.	2025-07-29	4.4
CVE-2025-43274	apple - macos	A privacy issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.6. A sandboxed process may be able to circumvent sandbox restrictions.	2025-07-30	4.4
CVE-2025-7738	red hat - multiple products	A flaw was found in Ansible Automation Platform (AAP) where the Gateway API returns the client secret for certain GitHub Enterprise authenticators in clear text. This vulnerability affects administrators or auditors accessing authenticator configurations. While access is limited to privileged users, the clear text exposure of sensitive credentials increases the risk of accidental leaks or misuse.	2025-07-31	4.4
CVE-2025-43228	apple - multiple products	The issue was addressed with improved UI. This issue is fixed in iOS 18.6 and iPadOS 18.6, Safari 18.6. Visiting a malicious website may lead to address bar spoofing.	2025-07-30	4.3
CVE-2025-43197	apple - multiple products	This issue was addressed with additional entitlement checks. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to access sensitive user data.	2025-07-30	4
CVE-2025-43206	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 15.6, macOS Ventura 13.7.7, macOS Sonoma 14.7.7. An app may be able to access protected user data.	2025-07-30	4
CVE-2025-43217	apple - multiple products	The issue was addressed by adding additional logic. This issue is fixed in iPadOS 17.7.9, iOS 18.6 and iPadOS 18.6. Privacy Indicators for microphone or camera access may not be correctly displayed.	2025-07-30	4
CVE-2025-43226	apple - multiple products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in watchOS 11.6, iOS 18.6 and iPadOS 18.6, iPadOS 17.7.9, tvOS 18.6, macOS Sequoia 15.6, macOS Sonoma 14.7.7, visionOS 2.6. Processing a maliciously crafted image may result in disclosure of process memory.	2025-07-30	4
CVE-2025-43230	apple - multiple products	The issue was addressed with additional permissions checks. This issue is fixed in iPadOS 17.7.9, watchOS 11.6, visionOS 2.6, iOS 18.6 and iPadOS 18.6, macOS Sequoia 15.6, tvOS 18.6. An app may be able to access user-sensitive data.	2025-07-30	4
CVE-2025-43250	apple - multiple products	A path handling issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to break out of its sandbox.	2025-07-30	4

CVE-2025-43265	apple - multiple products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in Safari 18.6, watchOS 11.6, visionOS 2.6, iOS 18.6 and iPadOS 18.6, macOS Sequoia 15.6, tvOS 18.6. Processing maliciously crafted web content may disclose internal states of the app.	2025-07-30	4
CVE-2025-8283	red hat - multiple products	A vulnerability was found in the netavark package, a network stack for containers used with Podman. Due to dns.podman search domain being removed, netavark may return external servers if a valid A/AAAA record is sent as a response. When creating a container with a given name, this name will be used as the hostname for the container itself, as the podman's search domain is not added anymore the container is using the host's resolv.conf, and the DNS resolver will try to look into the search domains contained on it. If one of the domains contain a name with the same hostname as the running container, the connection will forward to unexpected external servers.	2025-07-28	3.7
CVE-2025-37108	hewlett packard enterprise (hpe) - HPE Telco Service Activator	Cross-site scripting vulnerability has been identified in HPE Telco Service Activator product	2025-07-31	3.5
CVE-2025-37109	hewlett packard enterprise (hpe) - HPE Telco Service Activator	Cross-site scripting vulnerability has been identified in HPE Telco Service Activator product	2025-07-31	3.5
CVE-2025-36609	dell - smartfabric_os10	Dell SmartFabric OS10 Software, versions prior to 10.6.0.5, contains a Use of Hard-coded Password vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	2025-07-30	2.5

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.

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.