الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

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

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

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 ٢٠ يوليو إلى ٢٦ يوليو. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- عالي جدًا: النتيجة الأساسية 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

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 20th of July to 26th of July. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score
CVE-2025-41240	vmware - multiple products	Three Bitnami Helm charts mount Kubernetes Secrets under a predictable path (/opt/bitnami/*/secrets) that is located within the web server document root. In affected versions, this can lead to unauthenticated access to sensitive credentials via HTTP/S. A remote attacker could retrieve these secrets by accessing specific URLs if the application is exposed externally. The issue affects deployments using the default value of usePasswordFiles=true, which mounts secrets as files into the container filesystem.	2025-07-24	10
CVE-2025-53770	microsoft - multiple products	Deserialization of untrusted data in on-premises Microsoft SharePoint Server allows an unauthorized attacker to execute code over a network. Microsoft is aware that an exploit for CVE-2025-53770 exists in the wild. Microsoft is preparing and fully testing a comprehensive update to address this vulnerability. In the meantime, please make sure that the mitigation provided in this CVE documentation is in place so that you are protected from exploitation.	2025-07-20	9.8
CVE-2025-6704	sophos - Sophos Firewall	An arbitrary file writing vulnerability in the Secure PDF eXchange (SPX) feature of Sophos Firewall versions older than 21.0 MR2 (21.0.2) can lead to pre-auth remote code execution, if a specific configuration of SPX is enabled in combination with the firewall running in High Availability (HA) mode.	2025-07-21	9.8
CVE-2025-7624	sophos - Sophos Firewall	An SQL injection vulnerability in the legacy (transparent) SMTP proxy of Sophos Firewall versions older than 21.0 MR2 (21.0.2) can lead to remote code execution, if a quarantining policy is active for Email and SFOS was upgraded from a version older than 21.0 GA.	2025-07-21	9.8
CVE-2025-7393	drupal - Mail Login	Improper Restriction of Excessive Authentication Attempts vulnerability in Drupal Mail Login allows Brute Force.This issue affects Mail Login: from 3.0.0 before 3.2.0, from 4.0.0 before 4.2.0.	2025-07-21	9.8
CVE-2025-8028	mozilla - multiple products	On arm64, a WASM `br_table` instruction with a lot of entries could lead to the label being too far from the instruction causing truncation and incorrect computation of the branch address. This vulnerability affects Firefox < 141, Firefox ESR < 115.26, Firefox ESR < 128.13, Firefox ESR < 140.1, Thunderbird < 141, Thunderbird < 128.13, and Thunderbird < 140.1.	2025-07-22	9.8
CVE-2025-8031	mozilla - multiple products	The `username:password` part was not correctly stripped from URLs in CSP reports potentially leaking HTTP Basic Authentication credentials. This vulnerability affects Firefox < 141, Firefox ESR < 128.13, Firefox ESR < 140.1, Thunderbird < 141, Thunderbird < 128.13, and Thunderbird < 140.1.	2025-07-22	9.8
CVE-2025-8038	mozilla - multiple products	Firefox ignored paths when checking the validity of navigations in a frame. This vulnerability affects Firefox < 141, Firefox ESR < 140.1, Thunderbird < 141, and Thunderbird < 140.1.	2025-07-22	9.8
CVE-2025-8043	mozilla - multiple products	Focus incorrectly truncated URLs towards the beginning instead of around the origin. This vulnerability affects Firefox < 141 and Thunderbird < 141.	2025-07-22	9.8
CVE-2025-8044	mozilla - multiple products	Memory safety bugs present in Firefox 140 and Thunderbird 140. 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 < 141 and Thunderbird < 141.	2025-07-22	9.8
CVE-2025-54438	samsung - magicinfo_9_server	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Samsung Electronics MagicINFO 9 Server allows Upload a Web Shell to a Web Server.This issue affects MagicINFO 9 Server: less than 21.1080.0	2025-07-23	9.8
CVE-2025-54440	samsung - magicinfo_9_server	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	2025-07-23	9.8

CVE-2025-54442	samsung - magicinfo_9_server	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	2025-07-23	9.8
CVE-2025-54443	samsung - magicinfo_9_server	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Samsung Electronics MagicINFO 9 Server allows Upload a Web Shell to a Web Server.This issue affects MagicINFO 9 Server: less than 21.1080.0	2025-07-23	9.8
CVE-2025-54444	samsung - magicinfo_9_server	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	2025-07-23	9.8
CVE-2025-54446	samsung - magicinfo_9_server	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Samsung Electronics MagicINFO 9 Server allows Upload a Web Shell to a Web Server.This issue affects MagicINFO 9 Server: less than 21.1080.0	2025-07-23	9.8
CVE-2025-54448	samsung - magicinfo_9_server	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	2025-07-23	9.8
CVE-2025-54449	samsung - magicinfo_9_server	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	2025-07-23	9.8
CVE-2025-54451	samsung - magicinfo_9_server	Improper Control of Generation of Code ('Code Injection') vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	2025-07-23	9.8
CVE-2014-125117	d-link - DSP-W215	A stack-based buffer overflow vulnerability in the my_cgi.cgi component of certain D-Link devices, including the DSP-W215 version 1.02, can be exploited via a specially crafted HTTP POST request to the /common/info.cgi endpoint. This flaw enables an unauthenticated attacker to achieve remote code execution with system-level privileges.	2025-07-25	9.3
CVE-2025-8037	mozilla - multiple products	Setting a nameless cookie with an equals sign in the value shadowed other cookies. Even if the nameless cookie was set over HTTP and the shadowed cookie included the `Secure` attribute. This vulnerability affects Firefox < 141, Firefox ESR < 140.1, Thunderbird < 141, and Thunderbird < 140.1.	2025-07-22	9.1
CVE-2025-54454	samsung - magicinfo_9_server	Use of Hard-coded Credentials vulnerability in Samsung Electronics MagicINFO 9 Server allows Authentication Bypass.This issue affects MagicINFO 9 Server: less than 21.1080.0.	2025-07-23	9.1
CVE-2025-54455	samsung - magicinfo_9_server	Use of Hard-coded Credentials vulnerability in Samsung Electronics MagicINFO 9 Server allows Authentication Bypass.This issue affects MagicINFO 9 Server: less than 21.1080.0.	2025-07-23	9.1
CVE-2025-40599	sonicwall - SMA 100 Series	An authenticated arbitrary file upload vulnerability exists in the SMA 100 series web management interface. A remote attacker with administrative privileges can exploit this flaw to upload arbitrary files to the system, potentially leading to remote code execution.	2025-07-23	9.1
CVE-2025-50151	apache - jena	File access paths in configuration files uploaded by users with administrator access are not validated. This issue affects Apache Jena version up to 5.4.0. Users are recommended to upgrade to version 5.5.0, which does not allow arbitrary configuration upload.	2025-07-21	8.8
CVE-2025-7382	sophos - Sophos Firewall	A command injection vulnerability in WebAdmin of Sophos Firewall versions older than 21.0 MR2 (21.0.2) can lead to adjacent attackers achieving pre-auth code execution on High Availability (HA) auxiliary devices, if OTP authentication for the admin user is enabled.	2025-07-21	8.8
CVE-2025-8034	mozilla - multiple products	Memory safety bugs present in Firefox ESR 115.25, Firefox ESR 128.12, Thunderbird ESR 128.12, Firefox ESR 140.0, Thunderbird ESR 140.0, Firefox 140 and Thunderbird 140. 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 < 141, Firefox ESR < 115.26, Firefox ESR < 128.13, Firefox ESR < 140.1, Thunderbird < 141, Thunderbird < 128.13, and Thunderbird < 140.1.	2025-07-22	8.8
CVE-2025-8035	mozilla - multiple products	Memory safety bugs present in Firefox ESR 128.12, Thunderbird ESR 128.12, Firefox ESR 140.0, Thunderbird ESR 140.0, Firefox 140 and Thunderbird 140. 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 < 141, Firefox ESR < 128.13, Firefox ESR < 140.1, Thunderbird < 141, Thunderbird < 128.13, and Thunderbird < 140.1.	2025-07-22	8.8
CVE-2025-8040	mozilla - multiple products	Memory safety bugs present in Firefox ESR 140.0, Thunderbird ESR 140.0, Firefox 140 and Thunderbird 140. 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 < 141, Firefox ESR < 140.1, Thunderbird < 141, and Thunderbird < 140.1.	2025-07-22	8.8
CVE-2025-8010	google - chrome	Type Confusion in V8 in Google Chrome prior to 138.0.7204.168 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2025-07-22	8.8
CVE-2025-8011	google - chrome	Type Confusion in V8 in Google Chrome prior to 138.0.7204.168 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2025-07-22	8.8
CVE-2025-54439	samsung - magicinfo_9_server	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	2025-07-23	8.8
CVE-2025-54441	samsung - magicinfo_9_server	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	2025-07-23	8.8
CVE-2025-54453	samsung - magicinfo_9_server	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	2025-07-23	8.8
CVE-2025-33076	ibm - Engineering Systems Design Rhapsody	IBM Engineering Systems Design Rhapsody 9.0.2, 10.0, and 10.0.1 is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. A local user could overflow the buffer and execute arbitrary code on the system.	2025-07-23	8.8

CVE-2025-33077	ibm - Engineering Systems Design Rhapsody	IBM Engineering Systems Design Rhapsody 9.0.2, 10.0, and 10.0.1 is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. A local user could overflow the buffer and execute arbitrary code on the system.	2025-07-23	8.8
CVE-2025-7945	d-link - DIR-513	A vulnerability was found in D-Link DIR-513 up to 20190831. It has been declared as critical. This vulnerability affects the function formSetWanDhcpplus of the file /goform/formSetWanDhcpplus. The manipulation of the argument curTime leads to buffer overflow. The attack can be initiated remotely. This vulnerability only affects products that are no longer supported by the maintainer.	2025-07-22	8.7
CVE-2024-13974	sophos - Sophos Firewall	A business logic vulnerability in the Up2Date component of Sophos Firewall older than version 21.0 MR1 (20.0.1) can lead to attackers controlling the firewall's DNS environment to achieve remote code execution.	2025-07-21	8.1
CVE-2025-8029	mozilla - multiple products	Firefox executed `javascript:` URLs when used in `object` and `embed` tags. This vulnerability affects Firefox < 141, Firefox ESR < 128.13, Firefox ESR < 140.1, Thunderbird < 141, Thunderbird < 128.13, and Thunderbird < 140.1.	2025-07-22	8.1
CVE-2025-8030	mozilla - multiple products	Insufficient escaping in the "Copy as cURL" feature could potentially be used to trick a user into executing unexpected code. This vulnerability affects Firefox < 141, Firefox ESR < 128.13, Firefox ESR < 140.1, Thunderbird < 141, Thunderbird < 128.13, and Thunderbird < 140.1.	2025-07-22	8.1
CVE-2025-8032	mozilla - multiple products	XSLT document loading did not correctly propagate the source document which bypassed its CSP. This vulnerability affects Firefox < 141, Firefox ESR < 128.13, Firefox ESR < 140.1, Thunderbird < 141, Thunderbird < 128.13, and Thunderbird < 140.1.	2025-07-22	8.1
CVE-2025-8036	mozilla - multiple products	Firefox cached CORS preflight responses across IP address changes. This allowed circumventing CORS with DNS rebinding. This vulnerability affects Firefox < 141, Firefox ESR < 140.1, Thunderbird < 141, and Thunderbird < 140.1.	2025-07-22	8.1
CVE-2025-8039	mozilla - multiple products	In some cases search terms persisted in the URL bar even after navigating away from the search page. This vulnerability affects Firefox < 141, Firefox ESR < 140.1, Thunderbird < 141, and Thunderbird < 140.1.	2025-07-22	8.1
CVE-2025-54447	samsung - magicinfo_9_server	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	2025-07-23	8.1
CVE-2025-26397	solarwinds - SolarWinds Observability Self-Hosted	SolarWinds Observability Self-Hosted is susceptible to Deserialization of Untrusted Data Local Privilege Escalation vulnerability. An attacker with low privileges can escalate privileges to run malicious files copied to a permission-protected folder. This vulnerability requires authentication from a low-level account and local access to the host server.	2025-07-24	7.8
CVE-2025-49656	apache - jena	Users with administrator access can create databases files outside the files area of the Fuseki server. This issue affects Apache Jena version up to 5.4.0. Users are recommended to upgrade to version 5.5.0, which fixes the issue.	2025-07-21	7.5
CVE-2025-44649	trendnet - tew-wlc100p_firmware	In the configuration file of racoon in the TRENDnet TEW-WLC100P 2.03b03, the first item of exchage_mode is set to aggressive. Aggressive mode in IKE Phase 1 exposes identity information in plaintext, is vulnerable to offline dictionary attacks, and lacks flexibility in negotiating security parameters.	2025-07-21	7.5
CVE-2025-7717	drupal - File Download	Missing Authorization vulnerability in Drupal File Download allows Forceful Browsing.This issue affects File Download: from 0.0.0 before 1.9.0, from 2.0.0 before 2.0.1.	2025-07-21	7.5
CVE-2025-40597	sonicwall - SMA 100 Series	A Heap-based buffer overflow vulnerability in the SMA100 series web interface allows remote, unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution.	2025-07-23	7.5
CVE-2025-33109	ibm - i	IBM i 7.2, 7.3, 7.4, 7.5, and 7.6 is vulnerable to a privilege escalation caused by an invalid database authority check. A bad actor could execute a database procedure or function without having all required permissions, in addition to causing denial of service for some database actions.	2025-07-24	7.5
CVE-2025-7911	d-link - DI-8100	A vulnerability classified as critical was found in D-Link DI-8100 1.0. This vulnerability affects the function sprintf of the file /upnp_ctrl.asp of the component jhttpd. The manipulation of the argument remove_ext_proto/remove_ext_port leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2025-07-20	7.4
CVE-2025-8159	d-link - DIR-513	A vulnerability was found in D-Link DIR-513 1.0. It has been rated as critical. This issue affects the function formLanguageChange of the file /goform/formLanguageChange of the component HTTP POST Request Handler. The manipulation of the argument curTime leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	2025-07-25	7.4
CVE-2025-54452	samsung - magicinfo_9_server	Improper Authentication vulnerability in Samsung Electronics MagicINFO 9 Server allows Authentication Bypass.This issue affects MagicINFO 9 Server: less than 21.1080.0.	2025-07-23	7.3
CVE-2025-40596	sonicwall - SMA 100 Series	A Stack-based buffer overflow vulnerability in the SMA100 series web interface allows remote, unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution.	2025-07-23	7.3
CVE-2024-53286	synology - multiple products	Improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability in DDNS Record functionality in Synology Router Manager (SRM) before 1.3.1-9346-11 allows remote authenticated users with administrator privileges to execute arbitrary code via unspecified vectors.	2025-07-23	7.2
CVE-2025-54450	samsung - magicinfo_9_server	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	2025-07-23	7.2
CVE-2025-8175	d-link - DI-8400	A vulnerability was found in D-Link DI-8400 16.07.26A1. It has been classified as problematic. This affects an unknown part of the file usb_paswd.asp of the component jhttpd. The manipulation of the argument share_enable leads to null pointer dereference. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2025-07-26	7.1
CVE-2024-13973	sophos - Sophos Firewall	A post-auth SQL injection vulnerability in WebAdmin of Sophos Firewall versions older than 21.0 MR1 (21.0.1) can potentially lead to administrators achieving arbitrary code execution.	2025-07-21	6.8

CVE-2025-0664	trellix - Trellix Endpoint Security (HX) Agent	A locally authenticated, privileged user can craft a malicious OpenSSL configuration file, potentially leading the agent to load an arbitrary local library. This may impair endpoint defenses and allow the attacker to achieve code execution with SYSTEM-level privileges.	2025-07-21	6.7
CVE-2025-32744	dell - AppSync	Dell AppSync, version(s) 4.6.0.0, contains an Unrestricted Upload of File with Dangerous Type vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Remote execution.	2025-07-21	6.6
CVE-2025-53771	microsoft - multiple products	Improper authentication in Microsoft Office SharePoint allows an unauthorized attacker to perform spoofing over a network.	2025-07-20	6.5
CVE-2025-36106	ibm - Cognos Analytics Mobile	IBM Cognos Analytics Mobile (iOS) 1.1.0 through 1.1.22 could allow malicious actors to view and modify information coming to and from the application which could then be used to access confidential information on the device or network by using a the deprecated or misconfigured AFNetworking library at runtime.	2025-07-21	6.5
CVE-2025-8027	mozilla - multiple products	On 64-bit platforms IonMonkey-JIT only wrote 32 bits of the 64-bit return value space on the stack. Baseline-JIT, however, read the entire 64 bits. This vulnerability affects Firefox < 141, Firefox ESR < 115.26, Firefox ESR < 128.13, Firefox ESR < 140.1, Thunderbird < 141, Thunderbird < 128.13, and Thunderbird < 140.1.	2025-07-22	6.5
CVE-2025-8033	mozilla - multiple products	The JavaScript engine did not handle closed generators correctly and it was possible to resume them leading to a nullptr deref. This vulnerability affects Firefox < 141, Firefox ESR < 115.26, Firefox ESR < 128.13, Firefox ESR < 140.1, Thunderbird < 141, Thunderbird < 128.13, and Thunderbird < 140.1.	2025-07-22	6.5
CVE-2025-27930	manageengine - Applications Manager	Zohocorp ManageEngine Applications Manager versions 176600 and prior are vulnerable to stored cross-site scripting in the File/Directory monitor.	2025-07-23	6.4
CVE-2025-54090	apache software foundation - Apache HTTP Server	A bug in Apache HTTP Server 2.4.64 results in all "RewriteCond expr ..." tests evaluating as "true". Users are recommended to upgrade to version 2.4.65, which fixes the issue.	2025-07-23	6.3
CVE-2025-36116	ibm - Db2 Mirror for i	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 GUI is affected by cross-site WebSocket hijacking vulnerability. By sending a specially crafted request, an unauthenticated malicious actor could exploit this vulnerability to sniff an existing WebSocket connection to then remotely perform operations that the user is not allowed to perform.	2025-07-23	6.3
CVE-2025-36117	ibm - Db2 Mirror for i	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 does not disallow the session id after use which could allow an authenticated user to impersonate another user on the system.	2025-07-23	6.3
CVE-2024-40682	ibm - SmartCloud Analytics Log Analysis	IBM SmartCloud Analytics - Log Analysis 1.3.7.0, 1.3.7.1, 1.3.7.2, 1.3.8.0, 1.3.8.1, and 1.3.8.2 could allow a local user to cause a denial of service due to improper validation of specified type of input.	2025-07-23	6.2
CVE-2025-33013	ibm - multiple products	IBM MQ Operator LTS 2.0.0 through 2.0.29, MQ Operator CD 3.0.0, 3.0.1, 3.1.0 through 3.1.3, 3.3.0, 3.4.0, 3.4.1, 3.5.0, 3.5.1, 3.6.0, and MQ Operator SC2 3.2.0 through 3.2.13 Container could disclose sensitive information to a local user due to improper clearing of heap memory before release.	2025-07-24	6.2
CVE-2025-7392	drupal - Cookies Addons	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal Cookies Addons allows Cross-Site Scripting (XSS).This issue affects Cookies Addons: from 1.0.0 before 1.2.4.	2025-07-21	6.1
CVE-2025-7715	drupal - Block Attributes	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal Block Attributes allows Cross-Site Scripting (XSS).This issue affects Block Attributes: from 0.0.0 before 1.1.0, from 2.0.0 before 2.0.1.	2025-07-21	6.1
CVE-2025-7716	drupal - Real-time SEO for Drupal	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal Real-time SEO for Drupal allows Cross-Site Scripting (XSS).This issue affects Real-time SEO for Drupal: from 2.0.0 before 2.2.0.	2025-07-21	6.1
CVE-2025-40598	sonicwall - SMA 100 Series	A Reflected cross-site scripting (XSS) vulnerability exists in the SMA100 series web interface, allowing a remote unauthenticated attacker to potentially execute arbitrary JavaScript code.	2025-07-23	6.1
CVE-2025-36107	ibm - Cognos Analytics Mobile	IBM Cognos Analytics Mobile (iOS) 1.1.0 through 1.1.22 could allow malicious actors to obtain sensitive information due to the cleartext transmission of data.	2025-07-21	5.9
CVE-2025-36062	ibm - Cognos Analytics Mobile	IBM Cognos Analytics Mobile (iOS) 1.1.0 through 1.1.22 could be vulnerable to information exposure due to the use of unencrypted network traffic.	2025-07-21	5.9
CVE-2024-53287	synology - multiple products	Improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability in VPN Setting functionality in Synology Router Manager (SRM) before 1.3.1-9346-11 allows remote authenticated users with administrator privileges to inject arbitrary web script or HTML via unspecified vectors.	2025-07-23	5.9
CVE-2024-53288	synology - multiple products	Improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability in NTP Region functionality in Synology Router Manager (SRM) before 1.3.1-9346-11 allows remote authenticated users with administrator privileges to inject arbitrary web script or HTML via unspecified vectors.	2025-07-23	5.9
CVE-2025-33020	ibm - Engineering Systems Design Rhapsody	IBM Engineering Systems Design Rhapsody 9.0.2, 10.0, and 10.0.1 transmits sensitive information without encryption that could allow an attacker to obtain highly sensitive information.	2025-07-23	5.9
CVE-2025-36005	ibm - multiple products	IBM MQ Operator LTS 2.0.0 through 2.0.29, MQ Operator CD 3.0.0, 3.0.1, 3.1.0 through 3.1.3, 3.3.0, 3.4.0, 3.4.1, 3.5.0, 3.5.1, 3.6.0, and MQ Operator SC2 3.2.0 through 3.2.13 Internet Pass-Thru could allow a malicious user to obtain sensitive information from another TLS session connection by the proxy to the same hostname and port due to improper certificate validation.	2025-07-24	5.9
CVE-2025-22165	atlassian - sourcetree	This Medium severity ACE (Arbitrary Code Execution) vulnerability was introduced in version 4.2.8 of Sourcetree for Mac. This ACE (Arbitrary Code Execution) vulnerability, with a CVSS Score of 5.9, allows a locally authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires user interaction. Atlassian recommends that Sourcetree for Mac users upgrade to the latest version. If you are	2025-07-24	5.9

		unable to do so, upgrade your instance to one of the specified supported fixed versions. See the release notes https://www.sourcetreeapp.com/download-archives . You can download the latest version of Sourcetree for Mac from the download center https://www.sourcetreeapp.com/download-archives . This vulnerability was found through the Atlassian Bug Bounty Program by Karol Mazurek (AFINE).		
CVE-2024-41750	ibm - SmartCloud Analytics Log Analysis	IBM SmartCloud Analytics - Log Analysis 1.3.7.0, 1.3.7.1, 1.3.7.2, 1.3.8.0, 1.3.8.1, and 1.3.8.2 could allow a local, authenticated attacker to bypass client-side enforcement of security to manipulate data.	2025-07-23	5.5
CVE-2024-41751	ibm - SmartCloud Analytics Log Analysis	IBM SmartCloud Analytics - Log Analysis 1.3.7.0, 1.3.7.1, 1.3.7.2, 1.3.8.0, 1.3.8.1, and 1.3.8.2 could allow a local, authenticated attacker to bypass client-side enforcement of security to manipulate data.	2025-07-23	5.5
CVE-2025-8197	red hat - multiple products	A global buffer overflow vulnerability was found in the soup_header_name_to_string function in Libsoup. The `soup_header_name_to_string` function does not validate the `name` parameter passed in, and directly accesses `soup_header_name_strings[name]`. The value of `name` is controllable, when `name` exceeds the index range of `soup_headr_name_string`, it will cause an out-of-bounds access.	2025-07-25	5.5
CVE-2024-40686	ibm - SmartCloud Analytics Log Analysis	IBM SmartCloud Analytics - Log Analysis 1.3.7.0, 1.3.7.1, 1.3.7.2, 1.3.8.0, 1.3.8.1, and 1.3.8.2 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking.	2025-07-23	5.4
CVE-2025-46993	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.	2025-07-24	5.4
CVE-2025-46996	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.	2025-07-24	5.4
CVE-2025-47061	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.	2025-07-24	5.4
CVE-2025-7932	d-link - DIR-817L	A vulnerability classified as critical has been found in D-Link DIR-817L up to 1.04B01. This affects the function lxmldbc_system of the file ssdpcgi. The manipulation leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2025-07-21	5.3
CVE-2025-36057	ibm - Cognos Analytics Mobile	IBM Cognos Analytics Mobile (iOS) 1.1.0 through 1.1.22 is vulnerable to authentication bypass by using the Local Authentication Framework library which is not needed as biometric authentication is not used in the application.	2025-07-21	5.2
CVE-2025-8155	d-link - DCS-6010L	A vulnerability has been found in D-Link DCS-6010L 1.15.03 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /vb.htm of the component Management Application. The manipulation of the argument paratest leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	2025-07-25	5.1
CVE-2025-8114	red hat - multiple products	A flaw was found in libssh, a library that implements the SSH protocol. When calculating the session ID during the key exchange (KEX) process, an allocation failure in cryptographic functions may lead to a NULL pointer dereference. This issue can cause the client or server to crash.	2025-07-24	4.7
CVE-2024-38335	ibm - Security QRadar Network Threat Analytics	IBM Security QRadar Network Threat Analytics 1.0.0 through 1.3.1 could allow a privileged user to cause a denial of service due to improper allocation of resources.	2025-07-22	4.5
CVE-2025-30477	dell - PowerScale OneFS	Dell PowerScale OneFS, versions prior to 9.11.0.0, contains a use of a broken or risky cryptographic algorithm vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	2025-07-21	4.4
CVE-2025-36603	dell - AppSync	Dell AppSync, version(s) 4.6.0.0, contains an Improper Restriction of XML External Entity Reference vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure and Information tampering.	2025-07-21	4.2
CVE-2025-54352	wordpress - WordPress	WordPress 3.5 through 6.8.2 allows remote attackers to guess titles of private and draft posts via pingback.ping XML-RPC requests. NOTE: the Supplier is not changing this behavior.	2025-07-21	3.7

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.