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 ٢٩ يونيو إلى ٥ 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 29th of June to 5th 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-2025-34067	hikvision - Integrated Security Management Platform	An unauthenticated remote command execution vulnerability exists in the applyCT component of the Hikvision Integrated Security Management Platform due to the use of a vulnerable version of the Fastjson library. The endpoint /bic/ssoService/v1/applyCT deserializes untrusted user input, allowing an attacker to trigger Fastjson's auto-type feature to load arbitrary Java classes. By referencing a malicious class via an LDAP URL, an attacker can achieve remote code execution on the underlying system.	2025-07-02	10
CVE-2025-20309	cisco - multiple products	A vulnerability in Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an unauthenticated, remote attacker to log in to an affected device using the root account, which has default, static credentials that cannot be changed or deleted. This vulnerability is due to the presence of static user credentials for the root account that are reserved for use during development. An attacker could exploit this vulnerability by using the account to log in to an affected system. A successful exploit could allow the attacker to log in to the affected system and execute arbitrary commands as the root user.	2025-07-02	10
CVE-2025-34090	google - Chrome	A security bypass vulnerability exists in Google Chrome AppBound cookie encryption mechanism due to insufficient validation of COM server paths during inter-process communication. A local low-privileged attacker can hijack the COM class identifier (CLSID) registration used by Chrome's elevation service and point it to a non-existent or malicious binary. When this hijack occurs, Chrome silently falls back to the legacy cookie encryption mechanism (protected only by user-DPAPI), thereby enabling cookie decryption by any user-context malware without SYSTEM-level access. This flaw bypasses the protections intended by the AppBound encryption design and allows cookie theft from Chromium-based browsers. Confirmed in Google Chrome with AppBound Encryption enabled. Other Chromium-based browsers may be affected if they implement similar COM-based encryption mechanisms.	2025-07-02	9.3
CVE-2025-34092	google - Chrome	A cookie encryption bypass vulnerability exists in Google Chrome’s AppBound mechanism due to weak path validation logic within the elevation service. When Chrome encrypts a cookie key, it records its own executable path as validation metadata. Later, when decrypting, the elevation service compares the requesting process’s path to this stored path. However, due to path canonicalization inconsistencies, an attacker can impersonate Chrome (e.g., by naming their binary chrome.exe and placing it in a similar path) and successfully retrieve the encrypted cookie key. This allows malicious processes to retrieve cookies intended to be restricted to the Chrome process only. Confirmed in Google Chrome with AppBound Encryption enabled. Other Chromium-based browsers may be affected if they implement similar COM-based encryption mechanisms.	2025-07-02	9.3
CVE-2025-36593	dell - OpenManage Network Integration	Dell OpenManage Network Integration, versions prior to 3.8, contains an Authentication Bypass by Capture-replay vulnerability in the RADIUS protocol. An attacker with local network access could potentially exploit this vulnerability to forge a valid protocol accept message in response to a failed authentication request.	2025-06-30	8.8
CVE-2025-49520	red hat - multiple products	A flaw was found in Ansible Automation Platform’s EDA component where user-supplied Git URLs are passed unsanitized to the git ls-remote command. This vulnerability allows an authenticated attacker to inject arguments and execute arbitrary commands on the EDA worker. In	2025-06-30	8.8

		Kubernetes/OpenShift environments, this can lead to service account token theft and cluster access.		
CVE-2025-49521	red hat - multiple products	A flaw was found in the EDA component of the Ansible Automation Platform, where user-supplied Git branch or refspec values are evaluated as Jinja2 templates. This vulnerability allows authenticated users to inject expressions that execute commands or access sensitive files on the EDA worker. In OpenShift, it can lead to service account token theft.	2025-06-30	8.8
CVE-2025-49713	microsoft - edge_chromium	Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2025-07-02	8.8
CVE-2025-34091	google - Chrome	A padding oracle vulnerability exists in Google Chrome's AppBound cookie encryption mechanism due to observable decryption failure behavior in Windows Event Logs when handling malformed ciphertext in SYSTEM-DPAPI-encrypted blobs. A local attacker can repeatedly send malformed ciphertexts to the Chrome elevation service and distinguish between padding and MAC errors, enabling a padding oracle attack. This allows partial decryption of the SYSTEM-DPAPI layer and eventual recovery of the user-DPAPI encrypted cookie key, which is trivially decrypted by the attacker's own context. This issue undermines the core purpose of AppBound Encryption by enabling low-privileged cookie theft through cryptographic misuse and verbose error feedback. Confirmed in Google Chrome with AppBound Encryption enabled. Other Chromium-based browsers may be affected if they implement similar COM-based encryption mechanisms. This behavior arises from a combination of Chrome's AppBound implementation and the way Microsoft Windows DPAPI reports decryption failures via Event Logs. As such, the vulnerability relies on cryptographic behavior and error visibility in all supported versions of Windows.	2025-07-02	8.8
CVE-2025-6297	debian - dpkg	It was discovered that dpkg-deb does not properly sanitize directory permissions when extracting a control member into a temporary directory, which is documented as being a safe operation even on untrusted data. This may result in leaving temporary files behind on cleanup. Given automated and repeated execution of dpkg-deb commands on adversarial .deb packages or with well compressible files, placed inside a directory with permissions not allowing removal by a non-root user, this can end up in a DoS scenario due to causing disk quota exhaustion or disk full conditions.	2025-07-01	8.2
CVE-2025-6554	google - chrome	Type confusion in V8 in Google Chrome prior to 138.0.7204.96 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High)	2025-06-30	8.1
CVE-2025-6882	d-link - DIR-513	A vulnerability classified as critical has been found in D-Link DIR-513 1.0. This affects an unknown part of the file /goform/formSetWanPPTP. The manipulation of the argument curTime leads to buffer overflow. It is possible to initiate the attack 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.	2025-06-30	7.4
CVE-2025-49741	microsoft - edge_chromium	No cwe for this issue in Microsoft Edge (Chromium-based) allows an unauthorized attacker to disclose information over a network.	2025-07-01	7.4
CVE-2024-35164	apache - guacamole	The terminal emulator of Apache Guacamole 1.5.5 and older does not properly validate console codes received from servers via text-based protocols like SSH. If a malicious user has access to a text-based connection, a specially-crafted sequence of console codes could allow arbitrary code to be executed with the privileges of the running guacd process. Users are recommended to upgrade to version 1.6.0, which fixes this issue.	2025-07-02	6.8
CVE-2024-9453	red hat - OpenShift Developer Tools and Services	A vulnerability was found in Red Hat OpenShift Jenkins. The bearer token is not obfuscated in the logs and potentially carries a high risk if those logs are centralized when collected. The token is typically valid for one year. This flaw allows a malicious user to jeopardize the environment if they have access to sensitive information.	2025-07-04	6.5
CVE-2025-6931	d-link - multiple products	A vulnerability classified as problematic was found in D-Link DCS-6517 and DCS-7517 up to 2.02.0. Affected by this vulnerability is the function generate_pass_from_mac of the file /bin/httpd of the component Root Password Generation Handler. The manipulation leads to insufficient entropy. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. 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.	2025-06-30	6.3
CVE-2025-6932	d-link - DCS-7517	A vulnerability, which was classified as problematic, was found in D-Link DCS-7517 up to 2.02.0. This affects the function g_F_n_GenPassForQlync of the file /bin/httpd of the component Qlync Password Generation Handler. The manipulation leads to use of hard-coded password. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. 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.	2025-06-30	6.3
CVE-2025-2141	ibm - multiple products	IBM System Storage Virtualization Engine TS7700 3957 VED R5.4 8.54.2.17, R6.0 8.60.0.115, 3948 VED R5.4 8.54.2.17, R6.0 8.60.0.115, and 3948 VEF R6.0 8.60.0.115 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.	2025-07-01	6.1
CVE-2025-20310	cisco - Cisco Enterprise Chat and Email	A vulnerability in the web UI of Cisco Enterprise Chat and Email (ECE) could allow an unauthenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web UI does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the	2025-07-02	6.1

		affected interface or access sensitive, browser-based information. To successfully exploit this vulnerability, an attacker would need valid agent credentials.		
CVE-2025-20308	cisco - Cisco DNA Spaces Connector	A vulnerability in Cisco Spaces Connector could allow an authenticated, local attacker to elevate privileges and execute arbitrary commands on the underlying operating system as root. This vulnerability is due to insufficient restrictions during the execution of specific CLI commands. An attacker could exploit this vulnerability by logging in to the Cisco Spaces Connector CLI as the spacesadmin user and executing a specific command with crafted parameters. A successful exploit could allow the attacker to elevate privileges from the spacesadmin user and execute arbitrary commands on the underlying operating system as root.	2025-07-02	6
CVE-2025-6017	red hat - Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in Red Hat Advanced Cluster Management through versions 2.10, before 2.10.7, 2.11, before 2.11.4, and 2.12, before 2.12.4. This vulnerability allows an unprivileged user to view confidential managed cluster credentials through the UI. This information should only be accessible to authorized users and may result in the loss of confidentiality of administrative information, which could be leaked to unauthorized actors.	2025-07-02	5.5
CVE-2025-2895	ibm - Cloud Pak System	IBM Cloud Pak System 2.3.3.6, 2.3.36 iFix1, 2.3.3.7, 2.3.3.7 iFix1, 2.3.4.0, 2.3.4.1, and 2.3.4.1 iFix1 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.	2025-06-30	5.4
CVE-2025-36056	ibm - multiple products	IBM System Storage Virtualization Engine TS7700 3957 VED R5.4 8.54.2.17, R6.0 8.60.0.115, 3948 VED R5.4 8.54.2.17, R6.0 8.60.0.115, and 3948 VEF R6.0 8.60.0.115 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.	2025-07-01	5.4
CVE-2025-6896	d-link - DI-7300G+	A vulnerability classified as critical has been found in D-Link DI-7300G+ 19.12.25A1. Affected is an unknown function of the file wget_test.asp. The manipulation of the argument url leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2025-06-30	5.3
CVE-2025-6898	d-link - DI-7300G+	A vulnerability, which was classified as critical, has been found in D-Link DI-7300G+ 19.12.25A1. Affected by this issue is some unknown functionality of the file in proxy_client.asp. The manipulation of the argument proxy_srv/proxy_lanport/proxy_lanip/proxy_srvport leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2025-06-30	5.3
CVE-2025-6899	d-link - multiple products	A vulnerability, which was classified as critical, was found in D-Link DI-7300G+ and DI-8200G 17.12.20A1/19.12.25A1. This affects an unknown part of the file msp_info.htm. The manipulation of the argument flag/cmd/iface leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2025-06-30	5.3
CVE-2025-5967	trellix - Endpoint Security HX	A stored cross-site scripting vulnerability in ENS HX 10.0.4 allows a malicious user to inject arbitrary HTML into the ENS HX Malware Scan Name field, resulting in the exposure of sensitive data.	2025-07-01	5.3
CVE-2025-6920	red hat - multiple products	A flaw was found in the authentication enforcement mechanism of a model inference API in ai-inference-server. All /v1/* endpoints are expected to enforce API key validation. However, the POST /invocations endpoint failed to do so, resulting in an authentication bypass. This vulnerability allows unauthorized users to access the same inference features available on protected endpoints, potentially exposing sensitive functionality or allowing unintended access to backend resources.	2025-07-01	5.3
CVE-2025-46647	apache - apisix	A vulnerability of plugin openid-connect in Apache APISIX. This vulnerability will only have an impact if all of the following conditions are met: 1. Use the openid-connect plugin with introspection mode 2. The auth service connected to openid-connect provides services to multiple issuers 3. Multiple issuers share the same private key and relies only on the issuer being different If affected by this vulnerability, it would allow an attacker with a valid account on one of the issuers to log into the other issuer. This issue affects Apache APISIX: until 3.12.0. Users are recommended to upgrade to version 3.12.0 or higher.	2025-07-02	5.3
CVE-2025-6587	docker - Docker Desktop	System environment variables are recorded in Docker Desktop diagnostic logs, when using shell auto-completion. This leads to unintentional disclosure of sensitive information such as api keys, passwords, etc. A malicious actor with read access to these logs could obtain secrets and further use them to gain unauthorized access to other systems. Starting with version 4.43.0 Docker Desktop no longer logs system environment variables as part of diagnostics log collection.	2025-07-03	5.2
CVE-2025-0634	samsung - rlottie	Use After Free vulnerability in Samsung Open Source rLottie allows Remote Code Inclusion.This issue affects rLottie: V0.2.	2025-06-30	5.1
CVE-2025-53074	samsung - rlottie	Out-of-bounds Read vulnerability in Samsung Open Source rLottie allows Overflow Buffers.This issue affects rLottie: V0.2.	2025-06-30	5.1
CVE-2025-53076	samsung - rlottie	Improper Input Validation vulnerability in Samsung Open Source rLottie allows Overread Buffers.This issue affects rLottie: V0.2.	2025-06-30	5.1
CVE-2025-5372	red hat - multiple products	A flaw was found in libssh versions built with OpenSSL versions older than 3.0, specifically in the ssh_kdf() function responsible for key derivation. Due to inconsistent interpretation of return values where OpenSSL uses 0 to indicate failure and libssh uses 0 for success—the function may mistakenly return a success status even when key derivation fails. This results in uninitialized cryptographic key buffers being used in subsequent communication, potentially compromising SSH sessions' confidentiality, integrity, and availability.	2025-07-04	5

CVE-2025-36582	dell - NetWorker	Dell NetWorker, versions 19.12.0.1 and prior, contains a Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade') vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	2025-07-01	4.8
CVE-2025-20307	cisco - Cisco BroadWorks	A vulnerability in the web-based management interface of Cisco BroadWorks Application Delivery Platform could allow an authenticated, remote attacker to to conduct cross-site scripting (XSS) attacks against a user of the interface. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have valid administrative credentials.	2025-07-02	4.8
CVE-2025-6563	mikrotik - RouterOS	A cross-site scripting vulnerability is present in the hotspot of MikroTik's RouterOS on versions below 7.19.2. An attacker can inject the `javascript` protocol in the `dst` parameter. When the victim browses to the malicious URL and logs in, the XSS executes. The POST request used to login, can also be converted to a GET request, allowing an attacker to send a specifically crafted URL that automatically logs in the victim (into the attacker's account) and triggers the payload.	2025-07-03	4.8
CVE-2025-53075	samsung - rlottie	Improper Input Validation vulnerability in Samsung Open Source rLottie allows Path Traversal.This issue affects rLottie: V0.2.	2025-06-30	4.6
CVE-2025-5351	red hat - multiple products	A flaw was found in the key export functionality of libssh. The issue occurs in the internal function responsible for converting cryptographic keys into serialized formats. During error handling, a memory structure is freed but not cleared, leading to a potential double free issue if an additional failure occurs later in the function. This condition may result in heap corruption or application instability in low-memory scenarios, posing a risk to system reliability where key export operations are performed.	2025-07-04	4.2