الهيئــــة الوطنيــــة
للأمــــن السيبــــراني
National Cybersecurity Authority

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 15th of June to 21th of June. 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**

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 National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من 15 يونيو إلى 21 يونيو. 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**

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score
CVE-2025-23121	veeam - Backup and Recovery	A vulnerability allowing remote code execution (RCE) on the Backup Server by an authenticated domain user	2025-06-19	9.9
CVE-2025-47868	apache - nuttx	Out-of-bounds Write resulting in possible Heap-based Buffer Overflow vulnerability was discovered in tools/bdf-converter font conversion utility that is part of Apache NuttX RTOS repository. This standalone program is optional and neither part of NuttX RTOS nor Applications runtime, but active bdf-converter users may be affected when this tool is exposed to external provided user data data (i.e. publicly available automation). This issue affects Apache NuttX: from 6.9 before 12.9.0. Users are recommended to upgrade to version 12.9.0, which fixes the issue.	2025-06-16	9.8
CVE-2025-47869	apache - nuttx	Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability was discovered in Apache NuttX RTOS apps/exapmles/xmlrpc application. In this example application device stats structure that stored remotely provided parameters had hardcoded buffer size which could lead to buffer overflow. Structure members buffers were updated to valid size of CONFIG_XMLRPC_STRINGSIZE+1. This issue affects Apache NuttX RTOS users that may have used or base their code on example application as presented in releases from 6.22 before 12.9.0. Users of XMLRPC in Apache NuttX RTOS are advised to review their code for this pattern and update buffer sizes as presented in the version of the example in release 12.9.0.	2025-06-16	9.8
CVE-2025-6179	google - ChromeOS	Permissions Bypass in Extension Management in Google ChromeOS 16181.27.0 on managed Chrome devices allows a local attacker to disable extensions and access Developer Mode, including loading additional extensions via exploiting vulnerabilities using the ExtHang3r and ExtPrint3r tools.	2025-06-16	9.8
CVE-2025-45784	d-link - dph-400se_firmware	D-Link DPH-400S/SE VoIP Phone v1.01 contains hardcoded provisioning variables, including PROVIS_USER_PASSWORD, which may expose sensitive user credentials. An attacker with access to the firmware image can extract these credentials using static analysis tools such as strings or xxd, potentially leading to unauthorized access to device functions or user accounts. This vulnerability exists due to insecure storage of sensitive information in the firmware binary.	2025-06-18	9.8
CVE-2025-20260	cisco - ClamAV	A vulnerability in the PDF scanning processes of ClamAV could allow an unauthenticated, remote attacker to cause a buffer overflow condition, cause a denial of service (DoS) condition, or execute arbitrary code on an affected device. This vulnerability exists because memory buffers are allocated incorrectly when PDF files are processed. An attacker could exploit this vulnerability by submitting a crafted PDF file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to trigger a buffer overflow, likely resulting in the termination of the ClamAV scanning process and a DoS condition on the affected software. Although unproven, there is also a possibility that an attacker could leverage the buffer overflow to execute arbitrary code with the privileges of the ClamAV process.	2025-06-18	9.8
CVE-2024-53298	dell - PowerScale OneFS	Dell PowerScale OneFS, versions 9.5.0.0 through 9.10.0.1, contains a missing authorization vulnerability in the NFS export. An unauthenticated attacker with remote access could potentially exploit this vulnerability leading to unauthorized filesystem access. The attacker	2025-06-20	9.8

		may be able to read, modify, and delete arbitrary files. This vulnerability is considered critical as it can be leveraged to fully compromise the system. Dell recommends customers to upgrade at the earliest opportunity.		
CVE-2025-49794	red hat - multiple products	A use-after-free vulnerability was found in libxml2. This issue occurs when parsing XPath elements under certain circumstances when the XML schematron has the <sch:name path="..."/> schema elements. This flaw allows a malicious actor to craft a malicious XML document used as input for libxml, resulting in the program's crash using libxml or other possible undefined behaviors.	2025-06-16	9.1
CVE-2025-49796	red hat - multiple products	A vulnerability was found in libxml2. Processing certain sch:name elements from the input XML file can trigger a memory corruption issue. This flaw allows an attacker to craft a malicious XML input file that can lead libxml to crash, resulting in a denial of service or other possible undefined behavior due to sensitive data being corrupted in memory.	2025-06-16	9.1
CVE-2025-4404	red hat - multiple products	A privilege escalation from host to domain vulnerability was found in the FreeIPA project. The FreeIPA package fails to validate the uniqueness of the `krbCanonicalName` for the admin account by default, allowing users to create services with the same canonical name as the REALM admin. When a successful attack happens, the user can retrieve a Kerberos ticket in the name of this service, containing the admin@REALM credential. This flaw allows an attacker to perform administrative tasks over the REALM, leading to access to sensitive data and sensitive data exfiltration.	2025-06-17	9.1
CVE-2025-33117	ibm - QRadar SIEM	IBM QRadar SIEM 7.5 through 7.5.0 Update Package 12 could allow a privileged user to modify configuration files that would allow the upload of a malicious autoupdate file to execute arbitrary commands.	2025-06-19	9.1
CVE-2025-36049	ibm - webMethods Integration Server	IBM webMethods Integration Server 10.5, 10.7, 10.11, and 10.15 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote authenticated attacker could exploit this vulnerability to execute arbitrary commands.	2025-06-18	8.8
CVE-2025-6191	google - Chrome	Integer overflow in V8 in Google Chrome prior to 137.0.7151.119 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	2025-06-18	8.8
CVE-2025-6192	google - Chrome	Use after free in Metrics in Google Chrome prior to 137.0.7151.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2025-06-18	8.8
CVE-2025-3602	liferay - multiple products	Liferay Portal 7.4.0 through 7.4.3.97, and Liferay DXP 2023.Q3.1 through 2023.Q3.2, 7.4 GA through update 92, 7.3 GA through update 35, and 7.2 fix pack 8 through fix pack 20 does not limit the depth of a GraphQL queries, which allows remote attackers to perform denial-of-service (DoS) attacks on the application by executing complex queries.	2025-06-16	8.7
CVE-2025-3526	liferay - multiple products	SessionClicks in Liferay Portal 7.0.0 through 7.4.3.21, and Liferay DXP 7.4 GA through update 9, 7.3 GA through update 25, and older unsupported versions does not restrict the saving of request parameters in the HTTP session, which allows remote attackers to consume system memory leading to denial-of-service (DoS) conditions via crafted HTTP requests.	2025-06-16	8.7
CVE-2025-3594	liferay - multiple products	Path traversal vulnerability with the downloading and installation of Xuggler in Liferay Portal 7.0.0 through 7.4.3.4, and Liferay DXP 7.4 GA, 7.3 GA through update 34, and older unsupported versions allows remote attackers to (1) add files to arbitrary locations on the server and (2) download and execute arbitrary files from the download server via the `_com_liferay_server_admin_web_portlet_ServerAdminPortlet_jarName` parameter.	2025-06-16	8.6
CVE-2025-0320	citrix - Secure Access Client for Windows	Local Privilege escalation allows a low-privileged user to gain SYSTEM privileges in Citrix Secure Access Client for Windows	2025-06-17	8.6
CVE-2025-20271	cisco - Cisco Meraki MX Firmware	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition in the Cisco AnyConnect service on an affected device. This vulnerability is due to&nbsp;variable initialization errors when an SSL VPN session is established. An attacker could exploit this vulnerability by sending a sequence of crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of all established SSL VPN sessions and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established, effectively making the Cisco AnyConnect VPN service unavailable for all legitimate users.	2025-06-18	8.6
CVE-2025-49124	apache software foundation - Apache Tomcat	Untrusted Search Path vulnerability in Apache Tomcat installer for Windows. During installation, the Tomcat installer for Windows used icacls.exe without specifying a full path. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.7, from 10.1.0 through 10.1.41, from 9.0.23 through 9.0.105. Users are recommended to upgrade to version 11.0.8, 10.1.42 or 9.0.106, which fix the issue.	2025-06-16	8.4
CVE-2025-3319	ibm - Spectrum Protect Server	IBM Spectrum Protect Server 8.1 through 8.1.26 could allow attacker to bypass authentication due to improper session authentication which can result in access to unauthorized resources.	2025-06-20	8.1
CVE-2025-1411	ibm - Security Verify Directory	IBM Security Verify Directory Container 10.0.0.0 through 10.0.3.1 could allow a local user to execute commands as root due to execution with unnecessary privileges.	2025-06-15	7.8
CVE-2025-48976	apache software foundation - multiple products	Allocation of resources for multipart headers with insufficient limits enabled a DoS vulnerability in Apache Commons FileUpload. This issue affects Apache Commons FileUpload: from 1.0 before 1.6; from 2.0.0-M1 before 2.0.0-M4. Users are recommended to upgrade to versions 1.6 or 2.0.0-M4, which fix the issue.	2025-06-16	7.5
CVE-2025-48988	apache - multiple products	Allocation of Resources Without Limits or Throttling vulnerability in Apache Tomcat. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.7, from 10.1.0-M1 through 10.1.41, from 9.0.0.M1 through 9.0.105.	2025-06-16	7.5

		Users are recommended to upgrade to version 11.0.8, 10.1.42 or 9.0.106, which fix the issue.		
CVE-2025-49125	apache software foundation - Apache Tomcat	Authentication Bypass Using an Alternate Path or Channel vulnerability in Apache Tomcat. When using PreResources or PostResources mounted other than at the root of the web application, it was possible to access those resources via an unexpected path. That path was likely not to be protected by the same security constraints as the expected path, allowing those security constraints to be bypassed. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.7, from 10.1.0-M1 through 10.1.41, from 9.0.0.M1 through 9.0.105. Users are recommended to upgrade to version 11.0.8, 10.1.42 or 9.0.106, which fix the issue.	2025-06-16	7.5
CVE-2025-49795	red hat - multiple products	A NULL pointer dereference vulnerability was found in libxml2 when processing XPath XML expressions. This flaw allows an attacker to craft a malicious XML input to libxml2, leading to a denial of service.	2025-06-16	7.5
CVE-2025-33122	ibm - i	IBM i 7.2, 7.3, 7.4, 7.5, and 7.6 could allow a user to gain elevated privileges due to an unqualified library call in IBM Advanced Job Scheduler for i. A malicious actor could cause user-controlled code to run with administrator privilege.	2025-06-17	7.5
CVE-2025-31698	apache software foundation - Apache Traffic Server	ACL configured in ip_allow.config or remap.config does not use IP addresses that are provided by PROXY protocol. Users can use a new setting (proxy.config.acl.subjects) to choose which IP addresses to use for the ACL if Apache Traffic Server is configured to accept PROXY protocol. This issue affects undefined: from 10.0.0 through 10.0.6, from 9.0.0 through 9.2.10. Users are recommended to upgrade to version 9.2.11 or 10.0.6, which fixes the issue.	2025-06-19	7.5
CVE-2025-49763	apache software foundation - Apache Traffic Server	ESI plugin does not have the limit for maximum inclusion depth, and that allows excessive memory consumption if malicious instructions are inserted. Users can use a new setting for the plugin (--max-inclusion-depth) to limit it. This issue affects Apache Traffic Server: from 10.0.0 through 10.0.5, from 9.0.0 through 9.2.10. Users are recommended to upgrade to version 9.2.11 or 10.0.6, which fixes the issue.	2025-06-19	7.5
CVE-2025-49715	microsoft - Dynamics 365 FastTrack Implementation	Exposure of private personal information to an unauthorized actor in Dynamics 365 FastTrack Implementation Assets allows an unauthorized attacker to disclose information over a network.	2025-06-20	7.5
CVE-2025-3221	ibm - InfoSphere Information Server	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 could allow a remote attacker to cause a denial of service due to insufficient validation of incoming request resources.	2025-06-21	7.5
CVE-2025-6177	google - ChromeOS	Privilege Escalation in MiniOS in Google ChromeOS (16063.45.2 and potentially others) on enrolled devices allows a local attacker to gain root code execution via exploiting a debug shell (VT3 console) accessible through specific key combinations during developer mode entry and MiniOS access, even when developer mode is blocked by device policy or Firmware Write Protect (FWMP).	2025-06-16	7.4
CVE-2025-6151	tp-link - tl-wr940n_firmware	A vulnerability, which was classified as critical, has been found in TP-Link TL-WR940N V4. Affected by this issue is some unknown functionality of the file /userRpm/WanSlaacCfgRpm.htm. The manipulation of the argument dnsserver1 leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2025-06-17	7.4
CVE-2025-6158	d-link - DIR-665	A vulnerability classified as critical has been found in D-Link DIR-665 1.00. This affects the function sub_AC78 of the component HTTP POST Request Handler. The manipulation leads to stack-based 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.	2025-06-17	7.4
CVE-2025-6328	d-link - DIR-815	A vulnerability was found in D-Link DIR-815 1.01. It has been declared as critical. This vulnerability affects the function sub_403794 of the file hedwig.cgi. The manipulation leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2025-06-20	7.4
CVE-2025-6334	d-link - DIR-867	A vulnerability has been found in D-Link DIR-867 1.0 and classified as critical. This vulnerability affects the function strncpy of the component Query String Handler. The manipulation leads to stack-based buffer overflow. The attack can 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.	2025-06-20	7.4
CVE-2025-4879	citrix - Workspace App for Windows	Local Privilege escalation allows a low-privileged user to gain SYSTEM privileges in Citrix Workspace app for Windows	2025-06-17	7.3
CVE-2025-36048	ibm - webMethods Integration Server	IBM webMethods Integration Server 10.5, 10.7, 10.11, and 10.15 could allow a privileged user to escalate their privileges when handling external entities due to execution with unnecessary privileges.	2025-06-18	7.2
CVE-2025-24286	veeam - Backup and Recovery	A vulnerability allowing an authenticated user with the Backup Operator role to modify backup jobs, which could execute arbitrary code.	2025-06-19	7.2
CVE-2025-33121	ibm - QRadar SIEM	IBM QRadar SIEM 7.5 through 7.5.0 Update Package 12 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources.	2025-06-19	7.1
CVE-2025-6019	red hat - multiple products	A Local Privilege Escalation (LPE) vulnerability was found in libblockdev. Generally, the "allow_active" setting in Polkit permits a physically present user to take certain actions based on the session type. Due to the way libblockdev interacts with the udisks daemon, an "allow_active" user on a system may be able escalate to full root privileges on the target host.	2025-06-19	7

		Normally, udisks mounts user-provided filesystem images with security flags like nosuid and nodev to prevent privilege escalation. However, a local attacker can create a specially crafted XFS image containing a SUID-root shell, then trick udisks into resizing it. This mounts their malicious filesystem with root privileges, allowing them to execute their SUID-root shell and gain complete control of the system.		
CVE-2025-36016	ibm - Process Mining	IBM Process Mining 2.0.1 IF001 and 2.0.1 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.	2025-06-21	6.8
CVE-2025-49176	red hat - multiple products	A flaw was found in the Big Requests extension. The request length is multiplied by 4 before checking against the maximum allowed size, potentially causing an integer overflow and bypassing the size check.	2025-06-17	6.6
CVE-2025-49179	red hat - multiple products	A flaw was found in the X Record extension. The RecordSanityCheckRegisterClients function does not check for an integer overflow when computing request length, which allows a client to bypass length checks.	2025-06-17	6.6
CVE-2025-32896	apache software foundation - Apache SeaTunnel	# Summary Unauthorized users can perform Arbitrary File Read and Deserialization attack by submit job using restful api-v1. # Details Unauthorized users can access `/hazelcast/rest/maps/submit-job` to submit job. An attacker can set extra params in mysql url to perform Arbitrary File Read and Deserialization attack. This issue affects Apache SeaTunnel: <=2.3.10 # Fixed Users are recommended to upgrade to version 2.3.11, and enable restful api-v2 & open https two-way authentication , which fixes the issue.	2025-06-19	6.5
CVE-2025-36050	ibm - QRadar SIEM	IBM QRadar SIEM 7.5 through 7.5.0 Update Package 12 stores potentially sensitive information in log files that could be read by a local user.	2025-06-19	6.2
CVE-2025-49180	red hat - multiple products	A flaw was found in the RandR extension, where the RRChangeProviderProperty function does not properly validate input. This issue leads to an integer overflow when computing the total size to allocate.	2025-06-17	6.1
CVE-2025-24287	veeam - Backup for Microsoft Windows	A vulnerability allowing local system users to modify directory contents, allowing for arbitrary code execution on the local system with elevated permissions.	2025-06-19	6.1
CVE-2025-6193	red hat - multiple products	A command injection vulnerability was discovered in the TrustyAI Explainability toolkit. Arbitrary commands placed in certain fields of a LMEValJob custom resource (CR) may be executed in the LMEvalJob pod's terminal. This issue can be exploited via a maliciously crafted LMEvalJob by a user with permissions to deploy a CR.	2025-06-20	5.9
CVE-2025-5981	google - osv-scalibr	Arbitrary file write as the OSV-SCALIBR user on the host system via a path traversal vulnerability when using OSV-SCALIBR's unpack() function for container images. Particularly, when using the CLI flag --remote-image on untrusted container images.	2025-06-18	5.7
CVE-2025-49175	red hat - multiple products	A flaw was found in the X Rendering extension's handling of animated cursors. If a client provides no cursors, the server assumes at least one is present, leading to an out-of-bounds read and potential crash.	2025-06-17	5.5
CVE-2025-49177	red hat - multiple products	A flaw was found in the XFIXES extension. The XFixesSetClientDisconnectMode handler does not validate the request length, allowing a client to read unintended memory from previous requests.	2025-06-17	5.5
CVE-2025-49178	red hat - multiple products	A flaw was found in the X server's request handling. Non-zero 'bytes to ignore' in a client's request can cause the server to skip processing another client's request, potentially leading to a denial of service.	2025-06-17	5.5
CVE-2025-6196	red hat - Red Hat Enterprise Linux 7	A flaw was found in libgepub, a library used to read EPUB files. The software mishandles file size calculations when opening specially crafted EPUB files, leading to incorrect memory allocations. This issue causes the application to crash. Known affected usage includes desktop services like Tumbler, which may process malicious files automatically when browsing directories. While no direct remote attack vectors are confirmed, any application using libgepub to parse user-supplied EPUB content could be vulnerable to a denial of service.	2025-06-17	5.5
CVE-2025-1349	ibm - Sterling B2B Integrator	IBM Sterling B2B Integrator and IBM Sterling File Gateway 6.0.0.0 through 6.1.2.6 and 6.2.0.0 through 6.2.0.4 is vulnerable to stored cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-06-18	5.5
CVE-2024-54183	ibm - Sterling B2B Integrator	IBM Sterling B2B Integrator and IBM Sterling File Gateway 6.0.0.0 through 6.1.2.6 and 6.2.0.0 through 6.2.0.4 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.	2025-06-18	5.4
CVE-2025-20234	cisco - Cisco Secure Endpoint	A vulnerability in Universal Disk Format (UDF) processing of ClamAV could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to a memory overread during UDF file scanning. An attacker could exploit this vulnerability by submitting a crafted file containing UDF content to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to terminate the	2025-06-18	5.3

		ClamAV scanning process, resulting in a DoS condition on the affected software. For a description of this vulnerability, see the .		
CVE-2025-32753	dell - PowerScale OneFS	Dell PowerScale OneFS, versions 9.5.0.0 through 9.10.0.1, contains an improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to denial of service, information disclosure, and information tampering.	2025-06-20	5.3
CVE-2025-43200	apple - multiple products	This issue was addressed with improved checks. This issue is fixed in watchOS 11.3.1, macOS Ventura 13.7.4, iOS 15.8.4 and iPadOS 15.8.4, iOS 16.7.11 and iPadOS 16.7.11, iPadOS 17.7.5, visionOS 2.3.1, macOS Sequoia 15.3.1, iOS 18.3.1 and iPadOS 18.3.1, macOS Sonoma 14.7.4. A logic issue existed when processing a maliciously crafted photo or video shared via an iCloud Link. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals.	2025-06-16	4.8
CVE-2025-6141	gnu - ncurses	A vulnerability has been found in GNU ncurses up to 6.5-20250322 and classified as problematic. This vulnerability affects the function postprocess_termcap of the file tinfo/parse_entry.c. The manipulation leads to stack-based buffer overflow. The attack needs to be approached locally. Upgrading to version 6.5-20250329 is able to address this issue. It is recommended to upgrade the affected component.	2025-06-16	4.8
CVE-2025-36041	ibm - MQ Operator	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 through 3.5.3, and MQ Operator SC2 3.2.0 through 3.2.12 Native HA CRR could be configured with a private key and chain other than the intended key which could disclose sensitive information or allow the attacker to perform unauthorized actions.	2025-06-15	4.7
CVE-2024-54172	ibm - Sterling B2B Integrator	IBM Sterling B2B Integrator and IBM Sterling File Gateway 6.0.0.0 through 6.1.2.6 and 6.2.0.0 through 6.2.0.4 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.	2025-06-18	4.3
CVE-2025-3629	ibm - InfoSphere Information Server	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 could allow an authenticated user to delete another user's comments due to improper ownership management.	2025-06-21	4.3
CVE-2025-1348	ibm - Sterling B2B Integrator	IBM Sterling B2B Integrator and IBM Sterling File Gateway 6.0.0.0 through 6.1.2.6 and 6.2.0.0 through 6.2.0.4 could allow a local user to obtain sensitive information from a user's web browser cache due to not using a suitable caching policy.	2025-06-18	4
CVE-2025-6199	red hat - multiple products	A flaw was found in the GIF parser of GdkPixbuf's LZW decoder. When an invalid symbol is encountered during decompression, the decoder sets the reported output size to the full buffer length rather than the actual number of written bytes. This logic error results in uninitialized sections of the buffer being included in the output, potentially leaking arbitrary memory contents in the processed image.	2025-06-17	3.3
CVE-2025-1088	grafana - Grafana	In Grafana, an excessively long dashboard title or panel name will cause Chromium browsers to become unresponsive due to Improper Input Validation vulnerability in Grafana. This issue affects Grafana: before 11.6.2 and is fixed in 11.6.2 and higher.	2025-06-18	2.7
CVE-2025-5416	red hat - Red Hat Build of Keycloak	A vulnerability has been identified in Keycloak that could lead to unauthorized information disclosure. While it requires an already authenticated user, the /admin/serverinfo endpoint can inadvertently provide sensitive environment information.	2025-06-20	2.7
CVE-2025-6170	red hat - multiple products	A flaw was found in the interactive shell of the xmllint command-line tool, used for parsing XML files. When a user inputs an overly long command, the program does not check the input size properly, which can cause it to crash. This issue might allow attackers to run harmful code in rare configurations without modern protections.	2025-06-16	2.5

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.