الهيئـــة الوطنيـــة
للأمـــن السيبـــراني
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 20th of April to 26th of April. 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 20 أبريل إلى 26 أبريل. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score
CVE-2025-31324	sap - netweaver	SAP NetWeaver Visual Composer Metadata Uploader is not protected with a proper authorization, allowing unauthenticated agent to upload potentially malicious executable binaries that could severely harm the host system. This could significantly affect the confidentiality, integrity, and availability of the targeted system.	2025-04-24	10.0
CVE-2025-37087	hewlett packard enterprise (hpe) - HPE Performance Cluster Manager (HPCM)	A vulnerability in the cmdb service of the HPE Performance Cluster Manager (HPCM) could allow an attacker to gain access to an arbitrary file on the server host.	2025-04-22	9.8
CVE-2024-58250	samba - ppp	The passprompt plugin in pppd in ppp before 2.5.2 mishandles privileges.	2025-04-22	9.3
CVE-2025-1950	ibm - Hardware Management Console - Power Systems	IBM Hardware Management Console - Power Systems V10.2.1030.0 and V10.3.1050.0 could allow a local user to execute commands locally due to improper validation of libraries of an untrusted source.	2025-04-22	9.3
CVE-2025-1951	ibm - Hardware Management Console - Power Systems	IBM Hardware Management Console - Power Systems V10.2.1030.0 and V10.3.1050.0 could allow a local user to execute commands as a privileged user due to execution of commands with unnecessary privileges.	2025-04-22	8.4
CVE-2025-1731	zyxel - USG FLEX H series uOS firmware	An incorrect permission assignment vulnerability in the PostgreSQL commands of the USG FLEX H series uOS firmware versions from V1.20 through V1.31 could allow an authenticated local attacker with low privileges to gain access to the Linux shell and escalate their privileges by crafting malicious scripts or modifying system configurations with administrator-level access through a stolen token. Modifying the system configuration is only possible if the administrator has not logged out and the token remains valid.	2025-04-22	7.8
CVE-2025-1021	synology - DiskStation Manager (DSM)	Missing authorization vulnerability in synocopy in Synology DiskStation Manager (DSM) before 7.1.1-42962-8, 7.2.1-69057-7 and 7.2.2-72806-3 allows remote attackers to read arbitrary files via unspecified vectors.	2025-04-23	7.5
CVE-2025-32818	sonicwall - SonicOS	A Null Pointer Dereference vulnerability in the SonicOS SSLVPN Virtual office interface allows a remote, unauthenticated attacker to crash the firewall, potentially leading to a Denial-of-Service (DoS) condition.	2025-04-23	7.5
CVE-2025-27820	apache software foundation - Apache HttpComponents	A bug in PSL validation logic in Apache HttpClient 5.4.x disables domain checks, affecting cookie management and host name verification. Discovered by the Apache HttpClient team. Fixed in the 5.4.3 release	2025-04-24	7.5
CVE-2025-3903	drupal - UEditor	Vulnerability in Drupal UEdito. This issue affects UEditor*.*.	2025-04-23	7.3
CVE-2025-3904	drupal - Sportsleague	Vulnerability in Drupal Sportsleague. This issue affects Sportsleague: *.*.	2025-04-23	7.3
CVE-2025-37088	hewlett packard enterprise (hpe) - HPE Cray Data Virtualization Service (DVS)	A security vulnerability has been identified in HPE Cray Data Virtualization Service (DVS). Depending on race conditions and configuration, this vulnerability may lead to local/cluster unauthorized access.	2025-04-22	6.8
CVE-2025-2703	grafana - multiple products	The built-in XY Chart plugin is vulnerable to a DOM XSS vulnerability. A user with Editor permissions is able to modify such a panel in order to make it execute arbitrary JavaScript.	2025-04-23	6.8
CVE-2025-46421	red hat - multiple products	A flaw was found in libsoup. When libsoup clients encounter an HTTP redirect, they mistakenly send the HTTP Authorization header to the new host that the redirection points to. This allows the new host to impersonate the user to the original host that issued the redirect.	2025-04-24	6.8

CVE-2025-1732	zyxel - USG FLEX H series uOS firmware	An improper privilege management vulnerability in the recovery function of the USG FLEX H series uOS firmware version V1.31 and earlier could allow an authenticated local attacker with administrator privileges to upload a crafted configuration file and escalate privileges on a vulnerable device.	2025-04-22	6.7
CVE-2025-0618	trellix - FireEye EDR HX	A malicious third party could invoke a persistent denial of service vulnerability in FireEye EDR agent by sending a specially-crafted tamper protection event to the HX service to trigger an exception. This exception will prevent any further tamper protection events from being processed, even after a reboot of HX.	2025-04-23	6.5
CVE-2025-46420	red hat - multiple products	A flaw was found in libsoup. It is vulnerable to memory leaks in the soup_header_parse_quality_list() function when parsing a quality list that contains elements with all zeroes.	2025-04-24	6.5
CVE-2024-22351	ibm - InfoSphere Information Server	IBM InfoSphere Information 11.7 Server does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system.	2025-04-23	6.3
CVE-2025-3900	drupal - Colorbox	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal Colorbox allows Cross-Site Scripting (XSS). This issue affects Colorbox: from 0.0.0 before 2.1.3.	2025-04-23	6.1
CVE-2025-3901	drupal - Bootstrap Site Alert	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal Bootstrap Site Alert allows Cross-Site Scripting (XSS). This issue affects Bootstrap Site Alert: from 0.0.0 before 1.13.0, from 3.0.0 before 3.0.4.	2025-04-23	6.1
CVE-2025-3902	drupal - Block Class	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal Block Class allows Cross-Site Scripting (XSS). This issue affects Block Class: from 4.0.0 before 4.0.1.	2025-04-23	6.1
CVE-2025-43919	gnu - mailman	GNU Mailman 2.1.39, as bundled in cPanel (and WHM), allows unauthenticated attackers to read arbitrary files via ../ directory traversal at /mailman/private/mailman (aka the private archive authentication endpoint) via the username parameter. NOTE: multiple third parties report that they are unable to reproduce this, regardless of whether cPanel or WHM is used.	2025-04-20	5.8
CVE-2025-43716	ivanti - LANDesk Management Suite	A directory traversal vulnerability exists in Ivanti LANDesk Management Gateway through 4.2-1.9. By appending %3F.php to the URI of the /client/index.php endpoint, an attacker can bypass access controls and gain unauthorized access to various endpoints such as /client/index.php%3F.php/gsb/firewall.php within the management web panel, potentially exposing sensitive device information. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2025-04-23	5.8
CVE-2025-27087	hewlett packard enterprise (hpe) - HPE Cray Operating System (COS)	A vulnerability in the kernel of the Cray Operating System (COS) could allow an attacker to perform a local Denial of Service (DoS) attack.	2025-04-22	5.5
CVE-2025-2986	ibm - Maximo Asset Management	IBM Maximo Asset Management 7.6.1.3 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.	2025-04-25	5.5
CVE-2025-43920	gnu - mailman	GNU Mailman 2.1.39, as bundled in cPanel (and WHM), in certain external archiver configurations, allows unauthenticated attackers to execute arbitrary OS commands via shell metacharacters in an email Subject line. NOTE: multiple third parties report that they are unable to reproduce this, regardless of whether cPanel or WHM is used.	2025-04-20	5.4
CVE-2024-10306	red hat - multiple products	A vulnerability was found in mod_proxy_cluster. The issue is that the <Directory> directive should be replaced by the <Location> directive as the former does not restrict IP/host access as `Require ip IP_ADDRESS` would suggest. This means that anyone with access to the host might send MCMP requests that may result in adding/removing/updating nodes for the balancing. However, this host should not be accessible to the public network as it does not serve the general traffic.	2025-04-23	5.4
CVE-2025-43921	gnu - mailman	GNU Mailman 2.1.39, as bundled in cPanel (and WHM), allows unauthenticated attackers to create lists via the /mailman/create endpoint. NOTE: multiple third parties report that they are unable to reproduce this, regardless of whether cPanel or WHM is used.	2025-04-20	5.3
CVE-2025-3577	zyxel - AMG1302-T10B firmware	**UNSUPPORTED WHEN ASSIGNED** A path traversal vulnerability in the web management interface of the Zyxel AMG1302-T10B firmware version 2.00(AAJC.16)C0 could allow an authenticated attacker with administrator privileges to access restricted directories by sending a crafted HTTP request to an affected device.	2025-04-22	4.9
CVE-2025-3907	drupal - Search API Solr	Cross-Site Request Forgery (CSRF) vulnerability in Drupal Search API Solr allows Cross Site Request Forgery.This issue affects Search API Solr: from 0.0.0 before 4.3.9.	2025-04-23	4.3
CVE-2025-25045	ibm - InfoSphere Information Server	IBM InfoSphere Information 11.7 Server authenticated user to obtain sensitive information when a detailed technical error message is returned in a request. This information could be used in further attacks against the system.	2025-04-23	4.3
CVE-2025-27907	ibm - WebSphere Application Server	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	2025-04-22	4.1
CVE-2025-2987	ibm - Maximo Asset Management	IBM Maximo Asset Management 7.6.1.3 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	2025-04-22	3.8
CVE-2025-25046	ibm - InfoSphere Information Server	IBM InfoSphere Information Server 11.7 DataStage Flow Designer transmits sensitive information via URL or query parameters that could be exposed to an unauthorized actor using man in the middle techniques.	2025-04-23	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.