الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

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

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من ١٨ مايو إلى ٢٤ مايو. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

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

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 18th of May to 24th of May. 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-2024-6914	wso2 - multiple products	An incorrect authorization vulnerability exists in multiple WSO2 products due to a business logic flaw in the account recovery-related SOAP admin service. A malicious actor can exploit this vulnerability to reset the password of any user account, leading to a complete account takeover, including accounts with elevated privileges. This vulnerability is exploitable only through the account recovery SOAP admin services exposed via the "/services" context path in affected products. The impact may be reduced if access to these endpoints has been restricted based on the "Security Guidelines for Production Deployment" by disabling exposure to untrusted networks.	2025-05-22	9.8
CVE-2025-4978	netgear - DGND3700	A vulnerability, which was classified as very critical, was found in Netgear DGND3700 1.1.00.15_1.00.15NA. This affects an unknown part of the file /BRS_top.html of the component Basic Authentication. The manipulation leads to improper authentication. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Other products might be affected as well. The vendor was contacted early about this disclosure.	2025-05-20	9.3
CVE-2025-40634	tp-link - Link Archer AX50	Stack-based buffer overflow vulnerability in the 'conn-indicator' binary running as root on the TP-Link Archer AX50 router, in firmware versions prior to 1.0.15 build 241203 rel61480. This vulnerability allows an attacker to execute arbitrary code on the device over LAN and WAN networks.	2025-05-20	9.2
CVE-2025-24189	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in Safari 18.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. Processing maliciously crafted web content may lead to memory corruption.	2025-05-19	8.8
CVE-2025-47181	microsoft - Microsoft Edge (Chromium-based) Updater	Improper link resolution before file access ('link following') in Microsoft Edge (Chromium-based) allows an authorized attacker to elevate privileges locally.	2025-05-22	8.8
CVE-2025-4843	d-link - DCS-932L	A vulnerability was found in D-Link DCS-932L 2.18.01. It has been classified as critical. This affects the function SubUPnPCSInit of the file /sbin/udev. The manipulation of the argument CameraName 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.	2025-05-18	8.7
CVE-2022-31812	siemens - SiPass integrated	A vulnerability has been identified in SiPass integrated (All versions < V2.95.3.18). Affected server applications contain an out of bounds read past the end of an allocated buffer while checking the integrity of incoming packets. This could allow an unauthenticated remote attacker to create a denial of service condition.	2025-05-23	8.7
CVE-2025-20152	cisco - Cisco Identity Services Engine Software	A vulnerability in the RADIUS message processing feature of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper handling of certain RADIUS requests. An attacker could exploit this vulnerability by sending a specific authentication request to a network access device (NAD) that uses Cisco ISE for authentication, authorization, and accounting (AAA). A successful exploit could allow the attacker to cause Cisco ISE to reload.	2025-05-21	8.6
CVE-2025-3836	manageengine - ADAudit Plus	Zohocorp ManageEngine ADAudit Plus versions 8510 and prior are vulnerable to authenticated SQL injection in the logon events aggregate report.	2025-05-22	8.3

CVE-2025-41403	manageengine - ADAudit Plus	Zohocorp ManageEngine ADAudit Plus versions 8510 and prior are vulnerable to authenticated SQL injection while fetching service account audit data.	2025-05-22	8.3
CVE-2025-36527	manageengine - ADAudit Plus	Zohocorp ManageEngine ADAudit Plus versions below 8511 are vulnerable to SQL injection while exporting reports.	2025-05-23	8.3
CVE-2025-41407	manageengine - ADAudit Plus	Zohocorp ManageEngine ADAudit Plus versions below 8511 are vulnerable to SQL injection in the OU History report.	2025-05-23	8.3
CVE-2022-31807	siemens - multiple products	A vulnerability has been identified in SiPass integrated AC5102 (ACC-G2) (All versions), SiPass integrated ACC-AP (All versions). Affected devices do not properly check the integrity of firmware updates. This could allow a local attacker to upload a maliciously modified firmware onto the device. In a second scenario, a remote attacker who is able to intercept the transfer of a valid firmware from the server to the device could modify the firmware "on the fly".	2025-05-23	8.2
CVE-2025-4123	grafana - Grafana	A cross-site scripting (XSS) vulnerability exists in Grafana caused by combining a client path traversal and open redirect. This allows attackers to redirect users to a website that hosts a frontend plugin that will execute arbitrary JavaScript. This vulnerability does not require editor permissions and if anonymous access is enabled, the XSS will work. If the Grafana Image Renderer plugin is installed, it is possible to exploit the open redirect to achieve a full read SSRF. The default Content-Security-Policy (CSP) in Grafana will block the XSS though the `connect-src` directive.	2025-05-22	7.6
CVE-2025-4948	red hat - multiple products	A flaw was found in the soup_multipart_new_from_message() function of the libsoup HTTP library, which is commonly used by GNOME and other applications to handle web communications. The issue occurs when the library processes specially crafted multipart messages. Due to improper validation, an internal calculation can go wrong, leading to an integer underflow. This can cause the program to access invalid memory and crash. As a result, any application or server using libsoup could be forced to exit unexpectedly, creating a denial-of-service (DoS) risk.	2025-05-19	7.5
CVE-2025-4416	drupal - Events Log Track	Allocation of Resources Without Limits or Throttling vulnerability in Drupal Events Log Track allows Excessive Allocation.This issue affects Events Log Track: from 0.0.0 before 3.1.11, from 4.0.0 before 4.0.2.	2025-05-21	7.5
CVE-2025-5024	red hat - multiple products	A flaw was found in gnome-remote-desktop. Once gnome-remote-desktop listens for RDP connections, an unauthenticated attacker can exhaust system resources and repeatedly crash the process. There may be a resource leak after many attacks, which will also result in gnome-remote-desktop no longer being able to open files even after it is restarted via systemd.	2025-05-22	7.4
CVE-2025-22157	atlassian - multiple products	This High severity PrivEsc (Privilege Escalation) vulnerability was introduced in versions: 9.12.0, 10.3.0, 10.4.0, and 10.5.0 of Jira Core Data Center and Server 5.12.0, 10.3.0, 10.4.0, and 10.5.0 of Jira Service Management Data Center and Server This PrivEsc (Privilege Escalation) vulnerability, with a CVSS Score of 7.2, allows an attacker to perform actions as a higher-privileged user. Atlassian recommends that Jira Core Data Center and Server and Jira Service Management Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Jira Core Data Center and Server 9.12: Upgrade to a release greater than or equal to 9.12.20 Jira Service Management Data Center and Server 5.12: Upgrade to a release greater than or equal to 5.12.20 Jira Core Data Center 10.3: Upgrade to a release greater than or equal to 10.3.5 Jira Service Management Data Center 10.3: Upgrade to a release greater than or equal to 10.3.5 Jira Core Data Center 10.4: Upgrade to a release greater than or equal to 10.6.0 Jira Service Management Data Center 10.4: Upgrade to a release greater than or equal to 10.6.0 Jira Core Data Center 10.5: Upgrade to a release greater than or equal to 10.5.1 Jira Service Management Data Center 10.5: Upgrade to a release greater than or equal to 10.5.1 See the release notes. You can download the latest version of Jira Core Data Center and Jira Service Management Data Center from the download center. This vulnerability was reported via our Atlassian (Internal) program.	2025-05-20	7.2
CVE-2025-20113	cisco - multiple products	A vulnerability in Cisco Unified Intelligence Center could allow an authenticated, remote attacker to elevate privileges to Administrator for a limited set of functions on an affected system. This vulnerability is due to insufficient server-side validation of user-supplied parameters in API or HTTP requests. An attacker could exploit this vulnerability by submitting a crafted API or HTTP request to an affected system. A successful exploit could allow the attacker to access, modify, or delete data beyond the sphere of their intended access level, including obtaining potentially sensitive information stored in the system.	2025-05-21	7.1

CVE-2025-33136	ibm - aspera_faspex	IBM Aspera Faspex 5.0.0 through 5.0.12 could allow an authenticated user to obtain sensitive information or perform unauthorized actions on behalf of another user due to improper protection of assumed immutable data.	2025-05-22	7.1
CVE-2025-33137	ibm - aspera_faspex	IBM Aspera Faspex 5.0.0 through 5.0.12 could allow an authenticated user to obtain sensitive information or perform unauthorized actions on behalf of another user due to client-side enforcement of server-side security.	2025-05-22	7.1
CVE-2025-4977	netgear - DGND3700	A vulnerability, which was classified as problematic, has been found in Netgear DGND3700 1.1.00.15_1.00.15NA. Affected by this issue is some unknown functionality of the file /BRS_top.html. The manipulation leads to information disclosure. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Other products might be affected as well. The vendor was contacted early about this disclosure.	2025-05-20	6.9
CVE-2025-4980	netgear - DGND3700	A vulnerability has been found in Netgear DGND3700 1.1.00.15_1.00.15NA and classified as problematic. This vulnerability affects unknown code of the file /currentsetting.htm of the component mini_http. The manipulation leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Other products might be affected as well. The vendor was contacted early about this disclosure.	2025-05-20	6.9
CVE-2023-33861	ibm - Security ReaQta EDR	IBM Security ReaQta EDR 3.12 could allow an attacker to spoof a trusted entity by interfering with the communication path between the host and client.	2025-05-20	6.5
CVE-2024-45641	ibm - Security ReaQta EDR	IBM Security ReaQta EDR 3.12 could allow an attacker to perform unauthorized actions due to improper SSL certificate validation.	2025-05-20	6.5
CVE-2025-4969	red hat - multiple products	A vulnerability was found in the libsoup package. This flaw stems from its failure to correctly verify the termination of multipart HTTP messages. This can allow a remote attacker to send a specially crafted multipart HTTP body, causing the libsoup-consuming server to read beyond its allocated memory boundaries (out-of-bounds read).	2025-05-21	6.5
CVE-2025-20242	cisco - Cisco Unified Contact Center Enterprise	A vulnerability in the Cloud Connect component of Cisco Unified Contact Center Enterprise (CCE) could allow an unauthenticated, remote attacker to read and modify data on an affected device. This vulnerability is due to a lack of proper authentication controls. An attacker could exploit this vulnerability by sending crafted TCP data to a specific port on an affected device. A successful exploit could allow the attacker to read or modify data on the affected device.	2025-05-21	6.5
CVE-2025-20256	cisco - Cisco Secure Network Analytics	A vulnerability in the web-based management interface of Cisco Secure Network Analytics Manager and Cisco Secure Network Analytics Virtual Manager could allow an authenticated, remote attacker with valid administrative credentials to execute arbitrary commands as root on the underlying operating system. This vulnerability is due to insufficient input validation in specific fields of the web-based management interface. An attacker with valid administrative credentials could exploit this vulnerability by sending crafted input to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	2025-05-21	6.5
CVE-2025-20257	cisco - Cisco Secure Network Analytics	A vulnerability in an API subsystem of Cisco Secure Network Analytics Manager and Cisco Secure Network Analytics Virtual Manager could allow an authenticated, remote attacker with low privileges to generate fraudulent findings that are used to generate alarms and alerts on an affected product. Thi vulnerability is due to insufficient authorization enforcement on a specific API. An attacker could exploit this vulnerability by authenticating as a low-privileged user and performing API calls with crafted input. A successful exploit could allow the attacker to obfuscate legitimate findings in analytics reports or create false indications with alarms and alerts on an affected device.	2025-05-21	6.5
CVE-2025-3444	manageengine - multiple products	Zohocorp ManageEngine ServiceDesk Plus MSP and SupportCenter Plus versions below 14920 are vulnerable to authenticated Local File Inclusion (LFI) in the Admin module, where help card content is loaded.	2025-05-22	6.5
CVE-2025-4575	openssl - OpenSSL	Issue summary: Use of -addreject option with the openssl x509 application adds a trusted use instead of a rejected use for a certificate. Impact summary: If a user intends to make a trusted certificate rejected for a particular use it will be instead marked as trusted for that use. A copy & paste error during minor refactoring of the code introduced this issue in the OpenSSL 3.5 version. If, for example, a trusted CA certificate should be trusted only for the purpose of authenticating TLS servers but not for CMS signature verification and the CMS signature verification is intended to be marked as rejected with the -addreject option, the resulting CA certificate will be trusted for CMS signature verification purpose instead. Only users which use the trusted certificate format who use the openssl x509 command line application to add rejected uses are affected by this issue. The issues affecting only the command line application are considered to be Low severity. The FIPS modules in 3.5, 3.4, 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. OpenSSL 3.4, 3.3, 3.2, 3.1, 3.0, 1.1.1 and 1.0.2 are also not affected by this issue.	2025-05-22	6.5
CVE-2025-20246	cisco - Cisco Webex Meetings	A vulnerability in Cisco Webex could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack. A vulnerability is due to improper filtering of user-supplied input. An attacker could exploit this vulnerability by persuading a user to follow a malicious link. A successful exploit could allow the attacker to conduct a cross-site scripting attack against the targeted user.	2025-05-21	6.1

CVE-2025-20247	cisco - Cisco Webex Meetings	A vulnerability in Cisco Webex could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack. A vulnerability is due to improper filtering of user-supplied input. An attacker could exploit this vulnerability by persuading a user to follow a malicious link. A successful exploit could allow the attacker to conduct a cross-site scripting attack against the targeted user.	2025-05-21	6.1
CVE-2025-20250	cisco - Cisco Webex Meetings	A vulnerability in Cisco Webex could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack. A vulnerability is due to improper filtering of user-supplied input. An attacker could exploit this vulnerability by persuading a user to follow a malicious link. A successful exploit could allow the attacker to conduct a cross-site scripting attack against the targeted user.	2025-05-21	6.1
CVE-2024-5962	wso2 - multiple products	A reflected cross-site scripting (XSS) vulnerability exists in the authentication endpoint of multiple WSO2 products due to missing output encoding of user-supplied input. A malicious actor can exploit this vulnerability to inject arbitrary JavaScript into the authentication flow, potentially leading to UI modifications, redirections to malicious websites, or data exfiltration from the browser. While this issue could allow an attacker to manipulate the user's browser, session-related sensitive cookies remain protected with the httpOnly flag, preventing session hijacking.	2025-05-22	6.1
CVE-2024-7487	wso2 - multiple products	An improper authentication vulnerability exists in WSO2 Identity Server 7.0.0 due to an implementation flaw that allows app-native authentication to be bypassed when an invalid object is passed. Exploitation of this vulnerability could enable malicious actors to circumvent the client verification mechanism, compromising the integrity of the authentication process.	2025-05-22	5.8
CVE-2025-24183	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7.3, macOS Sequoia 15.3, macOS Sonoma 14.7.3. A local user may be able to modify protected parts of the file system.	2025-05-19	5.5
CVE-2025-24184	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in visionOS 2.3, iOS 18.3 and iPadOS 18.3, iPadOS 17.7.4, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. An app may be able to cause unexpected system termination.	2025-05-19	5.5
CVE-2025-31262	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. An app may be able to modify protected parts of the file system.	2025-05-19	5.5
CVE-2025-3580	grafana - Grafana	An access control vulnerability was discovered in Grafana OSS where an Organization administrator could permanently delete the Server administrator account. This vulnerability exists in the DELETE /api/org/users/ endpoint. The vulnerability can be exploited when: 1. An Organization administrator exists 2. The Server administrator is either: - Not part of any organization, or - Part of the same organization as the Organization administrator Impact: - Organization administrators can permanently delete Server administrator accounts - If the only Server administrator is deleted, the Grafana instance becomes unmanageable - No super-user permissions remain in the system - Affects all users, organizations, and teams managed in the instance The vulnerability is particularly serious as it can lead to a complete loss of administrative control over the Grafana instance.	2025-05-23	5.5
CVE-2025-20258	cisco - Cisco Duo	A vulnerability in the self-service portal of Cisco Duo could allow an unauthenticated, remote attacker to inject arbitrary commands into emails that are sent by the service. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by injecting arbitrary commands into a portion of an email that is sent by the service. A successful exploit could allow the attacker to send emails that contain malicious content to unsuspecting users.	2025-05-21	5.4
CVE-2025-33138	ibm - aspera_faspex	IBM Aspera Faspex 5.0.0 through 5.0.12 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.	2025-05-22	5.4
CVE-2025-20112	cisco - multiple products	A vulnerability in multiple Cisco Unified Communications and Contact Center Solutions products could allow an authenticated, local attacker to elevate privileges to root on an affected device.This vulnerability is due to excessive permissions that have been assigned to system commands. An attacker could exploit this vulnerability by executing crafted commands on the underlying operating system. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of an affected device. To successfully exploit this vulnerability, an attacker would need administrative access to the ESXi hypervisor.	2025-05-21	5.1
CVE-2025-5001	gnu - PSPP	A vulnerability was found in GNU PSPP 82fb509fb2fedd33e7ac0c46ca99e108bb3bdffb. It has been declared as problematic. This vulnerability affects the function calloc of the file pspp-convert.c. The manipulation of the argument -l leads to integer overflow. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used.	2025-05-20	4.8

CVE-2025-20267	cisco - Cisco Identity Services Engine Software	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker 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.	2025-05-21	4.8
CVE-2025-48010	drupal - One Time Password	Authentication Bypass Using an Alternate Path or Channel vulnerability in Drupal One Time Password allows Functionality Bypass.This issue affects One Time Password: from 0.0.0 before 1.3.0.	2025-05-21	4.8
CVE-2025-48011	drupal - One Time Password	Authentication Bypass Using an Alternate Path or Channel vulnerability in Drupal One Time Password allows Functionality Bypass.This issue affects One Time Password: from 0.0.0 before 1.3.0.	2025-05-21	4.8
CVE-2025-48012	drupal - One Time Password	Authentication Bypass by Capture-replay vulnerability in Drupal One Time Password allows Remote Services with Stolen Credentials.This issue affects One Time Password: from 0.0.0 before 1.3.0.	2025-05-21	4.8
CVE-2025-4415	drupal - Piwik PRO	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal Piwik PRO allows Cross-Site Scripting (XSS).This issue affects Piwik PRO: from 0.0.0 before 1.3.2.	2025-05-21	4.8
CVE-2024-7103	wso2 - WSO2 Identity Server	A reflected cross-site scripting (XSS) vulnerability exists in the sub-organization login flow of WSO2 Identity Server 7.0.0 due to improper input validation. A malicious actor can exploit this vulnerability to inject arbitrary JavaScript into the login flow, potentially leading to UI modifications, redirections to malicious websites, or data exfiltration from the browser. While this issue could allow an attacker to manipulate the user's browser, session-related sensitive cookies remain protected with the httpOnly flag, preventing session hijacking.	2025-05-22	4.6
CVE-2025-20114	cisco - multiple products	A vulnerability in the API of Cisco Unified Intelligence Center could allow an authenticated, remote attacker to perform a horizontal privilege escalation attack on an affected system. This vulnerability is due to insufficient validation of user-supplied parameters in API requests. An attacker could exploit this vulnerability by submitting crafted API requests to an affected system to execute an insecure direct object reference attack. A successful exploit could allow the attacker to access specific data that is associated with different users on the affected system.	2025-05-21	4.3
CVE-2025-20255	cisco - Cisco Webex Meetings	A vulnerability in client join services of Cisco Webex Meetings could allow an unauthenticated, remote attacker to manipulate cached HTTP responses within the meeting join service. This vulnerability is due to improper handling of malicious HTTP requests to the affected service. An attacker could exploit this vulnerability by manipulating stored HTTP responses within the service, also known as HTTP cache poisoning. A successful exploit could allow the attacker to cause the Webex Meetings service to return incorrect HTTP responses to clients.	2025-05-21	4.3
CVE-2025-5020	mozilla - Firefox for iOS	Opening maliciously-crafted URLs in Firefox from other apps such as Safari could have allowed attackers to spoof website addresses if the URLs utilized non-HTTP schemes used internally by the Firefox iOS client This vulnerability affects Firefox for iOS < 139.	2025-05-21	4.3
CVE-2025-4945	red hat - multiple products	A flaw was found in the cookie parsing logic of the libsoup HTTP library, used in GNOME applications and other software. The vulnerability arises when processing the expiration date of cookies, where a specially crafted value can trigger an integer overflow. This may result in undefined behavior, allowing an attacker to bypass cookie expiration logic, causing persistent or unintended cookie behavior. The issue stems from improper validation of large integer inputs during date arithmetic operations within the cookie parsing routines.	2025-05-19	3.7
CVE-2025-31185	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in iOS 18.3 and iPadOS 18.3. Photos in the Hidden Photos Album may be viewed without authentication.	2025-05-19	3.3
CVE-2025-48009	drupal - Single Content Sync	Missing Authorization vulnerability in Drupal Single Content Sync allows Functionality Misuse.This issue affects Single Content Sync: from 0.0.0 before 1.4.12.	2025-05-21	3.1