الهيئة الوطنية للأمن السيبراني
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.

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

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 26th of November to 2nd of December. 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**

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 ٢٦ نوفمبر إلى ٢ ديسمبر. 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	Severity
CVE-2023-49654	jenkins - matlab	Missing permission checks in Jenkins MATLAB Plugin 2.11.0 and earlier allow attackers to have Jenkins parse an XML file from the Jenkins controller file system.	2023-11-29	9.8	Critical
CVE-2023-49656	jenkins - matlab	Jenkins MATLAB Plugin 2.11.0 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	2023-11-29	9.8	Critical
CVE-2022-42536	google - android	Remote code execution	2023-11-29	9.8	Critical
CVE-2022-42537	google - android	Remote code execution	2023-11-29	9.8	Critical
CVE-2022-42538	google - android	Elevation of privilege	2023-11-29	9.8	Critical
CVE-2022-42540	google - android	Elevation of privilege	2023-11-29	9.8	Critical
CVE-2022-42541	google - android	Remote code execution	2023-11-29	9.8	Critical
CVE-2023-49693	netgear - prosafe_network_management_system	NETGEAR ProSAFE Network Management System has Java Debug Wire Protocol (JDWP) listening on port 11611 and it is remotely accessible by unauthenticated users, allowing attackers to execute arbitrary code.	2023-11-29	9.8	Critical
CVE-2023-35138	zyxel - nas326_firmware	A command injection vulnerability in the “show_zysync_server_contents” function of the Zyxel NAS326 firmware version V5.21(AAZF.14)C0 and NAS542 firmware version V5.21(ABAG.11)C0 could allow an unauthenticated attacker to execute some operating system (OS) commands by sending a crafted HTTP POST request.	2023-11-30	9.8	Critical
CVE-2023-4473	zyxel - nas326_firmware	A command injection vulnerability in the web server of the Zyxel NAS326 firmware version V5.21(AAZF.14)C0 and NAS542 firmware version V5.21(ABAG.11)C0 could allow an unauthenticated attacker to execute some operating system (OS) commands by sending a crafted URL to a vulnerable device.	2023-11-30	9.8	Critical
CVE-2023-4474	zyxel - nas326_firmware	The improper neutralization of special elements in the WSGI server of the Zyxel NAS326 firmware version V5.21(AAZF.14)C0 and NAS542 firmware version V5.21(ABAG.11)C0 could allow an unauthenticated attacker to execute some operating system (OS) commands by sending a crafted URL to a vulnerable device.	2023-11-30	9.8	Critical
CVE-2022-45135	apache - cocoon	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Apache Cocoon.This issue affects Apache Cocoon: from 2.2.0 before 2.3.0. Users are recommended to upgrade to version 2.3.0, which fixes the issue.	2023-11-30	9.8	Critical
CVE-2023-49733	apache - cocoon	Improper Restriction of XML External Entity Reference vulnerability in Apache Cocoon.This issue affects Apache Cocoon: from 2.2.0 before 2.3.0. Users are recommended to upgrade to version 2.3.0, which fixes the issue.	2023-11-30	9.8	Critical
CVE-2023-6345	google - chrome	Integer overflow in Skia in Google Chrome prior to 119.0.6045.199 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a malicious file. (Chromium security severity: High)	2023-11-29	9.6	Critical

CVE-2023-40610	apache - superset	Improper authorization check and possible privilege escalation on Apache Superset up to but excluding 2.1.2. Using the default examples database connection that allows access to both the examples schema and Apache Superset's metadata database, an attacker using a specially crafted CTE SQL statement could change data on the metadata database. This weakness could result on tampering with the authentication/authorization data.	2023-11-27	8.8	High
CVE-2023-42004	ibm - multiple products	IBM Security Guardium 11.3, 11.4, and 11.5 is potentially vulnerable to CSV injection. A remote attacker could execute malicious commands due to improper validation of csv file contents. IBM X-Force ID: 265262.	2023-11-28	8.8	High
CVE-2022-41678	apache - multiple products	Once an user is authenticated on Jolokia, he can potentially trigger arbitrary code execution. In details, in ActiveMQ configurations, jetty allows org.jolokia.http.AgentServlet to handler request to /api/jolokia org.jolokia.http.HttpRequestHandler#handlePostRequest is able to create JmxRequest through JSONObject. And calls to org.jolokia.http.HttpRequestHandler#executeRequest. Into deeper calling stacks, org.jolokia.handler.ExecHandler#doHandleRequest is able to invoke through refection. And then, RCE is able to be achieved via jdk.management.jfr.FlightRecorderMXBeanImpl which exists on Java version above 11. 1 Call newRecording. 2 Call setConfiguration. And a webshell data hides in it. 3 Call startRecording. 4 Call copyTo method. The webshell will be written to a .jsp file. The mitigation is to restrict (by default) the actions authorized on Jolokia, or disable Jolokia. A more restrictive Jolokia configuration has been defined in default ActiveMQ distribution. We encourage users to upgrade to ActiveMQ distributions version including updated Jolokia configuration: 5.16.6, 5.17.4, 5.18.0, 6.0.0.	2023-11-28	8.8	High
CVE-2023-40056	solarwinds - solarwinds_platform	SQL Injection Remote Code Vulnerability was found in the SolarWinds Platform. This vulnerability can be exploited with a low privileged account.	2023-11-28	8.8	High
CVE-2023-6346	google - chrome	Use after free in WebAudio in Google Chrome prior to 119.0.6045.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-11-29	8.8	High
CVE-2023-6347	google - chrome	Use after free in Mojo in Google Chrome prior to 119.0.6045.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-11-29	8.8	High
CVE-2023-6348	google - chrome	Type Confusion in Spellcheck in Google Chrome prior to 119.0.6045.199 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-11-29	8.8	High
CVE-2023-6350	google - chrome	Use after free in libavif in Google Chrome prior to 119.0.6045.199 allowed a remote attacker to potentially exploit heap corruption via a crafted avif file. (Chromium security severity: High)	2023-11-29	8.8	High

CVE-2023-6351	google - chrome	Use after free in libavif in Google Chrome prior to 119.0.6045.199 allowed a remote attacker to potentially exploit heap corruption via a crafted avif file. (Chromium security severity: High)	2023-11-29	8.8	High
CVE-2023-49655	jenkins - matlab	A cross-site request forgery (CSRF) vulnerability in Jenkins MATLAB Plugin 2.11.0 and earlier allows attackers to have Jenkins parse an XML file from the Jenkins controller file system.	2023-11-29	8.8	High
CVE-2023-49673	jenkins - neuvector_vulnerability_scanner	A cross-site request forgery (CSRF) vulnerability in Jenkins NeuVector Vulnerability Scanner Plugin 1.22 and earlier allows attackers to connect to an attacker-specified hostname and port using attacker-specified username and password.	2023-11-29	8.8	High
CVE-2023-37927	zyxel - nas326_firmware	The improper neutralization of special elements in the CGI program of the Zyxel NAS326 firmware version V5.21(AAZF.14)C0 and NAS542 firmware version V5.21(ABAG.11)C0 could allow an authenticated attacker to execute some operating system (OS) commands by sending a crafted URL to a vulnerable device.	2023-11-30	8.8	High
CVE-2023-37928	zyxel - nas326_firmware	A post-authentication command injection vulnerability in the WSGI server of the Zyxel NAS326 firmware version V5.21(AAZF.14)C0 and NAS542 firmware version V5.21(ABAG.11)C0 could allow an authenticated attacker to execute some operating system (OS) commands by sending a crafted URL to a vulnerable device.	2023-11-30	8.8	High
CVE-2023-42917	apple - multiple products	A memory corruption vulnerability was addressed with improved locking. This issue is fixed in iOS 17.1.2 and iPadOS 17.1.2, macOS Sonoma 14.1.2, Safari 17.1.2. Processing web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been exploited against versions of iOS before iOS 16.7.1.	2023-11-30	8.8	High
CVE-2023-38268	ibm - multiple products	IBM InfoSphere Information Server 11.7 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. IBM X-Force ID: 260585.	2023-12-01	8.8	High
CVE-2023-49694	netgear - prosafe_network_management_system	A low-privileged OS user with access to a Windows host where NETGEAR ProSAFE Network Management System is installed can create arbitrary JSP files in a Tomcat web application directory. The user can then execute the JSP files under the security context of SYSTEM.	2023-11-29	7.8	High
CVE-2023-45168	ibm - multiple products	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the invscout command to execute arbitrary commands. IBM X-Force ID: 267966.	2023-12-01	7.8	High
CVE-2023-39256	dell - rugged_control_center	Dell Rugged Control Center, version prior to 4.7, contains an improper access control vulnerability. A local malicious standard user could potentially exploit this vulnerability to modify the content in an unsecured folder during product installation and upgrade, leading to privilege escalation on the system.	2023-12-02	7.8	High
CVE-2023-39257	dell - rugged_control_center	Dell Rugged Control Center, version prior to 4.7, contains an Improper Access Control vulnerability. A local malicious standard user could potentially exploit this vulnerability to modify the content in an unsecured folder when product installation repair is performed, leading to privilege escalation on the system.	2023-12-02	7.8	High
CVE-2023-49068	apache - dolphinscheduler	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache DolphinScheduler.This issue affects Apache DolphinScheduler: before 3.2.1. Users are recommended to upgrade to version 3.2.1, which fixes the issue. At the time of disclosure of this advisory, this version has not yet been released. In the mean time, we recommend you make sure the logs are only available to trusted operators.	2023-11-27	7.5	High
CVE-2023-5871	redhat - multiple products	A flaw was found in libnbd, due to a malicious Network Block Device (NBD), a protocol for accessing Block Devices such as hard disks over a Network. This issue may allow a malicious NBD server to cause a Denial of Service.	2023-11-27	7.5	High
CVE-2023-4398	zyxel - zld	An integer overflow vulnerability in the source code of the QuickSec IPSec toolkit used in the VPN feature of the Zyxel ATP series firmware versions 4.32 through 5.37, USG FLEX series firmware versions 4.50 through 5.37, USG FLEX 50(W) series firmware versions 4.16 through 5.37, USG20(W)-VPN series firmware versions 4.16 through 5.37, and VPN series firmware versions 4.30 through 5.37, could allow an unauthenticated attacker to cause denial-of-service (DoS) conditions on an affected device by sending a crafted IKE packet.	2023-11-28	7.5	High
CVE-2023-34053	vmware - spring_framework	In Spring Framework versions 6.0.0 - 6.0.13, it is possible for a user to provide specially crafted HTTP requests that may cause a denial-of-service (DoS) condition.	2023-11-28	7.5	High

		Specifically, an application is vulnerable when all of the following are true: * the application uses Spring MVC or Spring WebFlux * io.micrometer:micrometer-core is on the classpath * an ObservationRegistry is configured in the application to record observations Typically, Spring Boot applications need the org.springframework.boot:spring-boot-actuator dependency to meet all conditions.			
CVE-2023-46589	apache - multiple products	Improper Input Validation vulnerability in Apache Tomcat.Tomcat from 11.0.0-M1 through 11.0.0-M10, from 10.1.0-M1 through 10.1.15, from 9.0.0-M1 through 9.0.82 and from 8.5.0 through 8.5.95 did not correctly parse HTTP trailer headers. A trailer header that exceeded the header size limit could cause Tomcat to treat a single request as multiple requests leading to the possibility of request smuggling when behind a reverse proxy. Users are recommended to upgrade to version 11.0.0-M11 onwards, 10.1.16 onwards, 9.0.83 onwards or 8.5.96 onwards, which fix the issue.	2023-11-28	7.5	High
CVE-2022-42539	google - android	Information disclosure	2023-11-29	7.5	High
CVE-2023-35137	zyxel - nas326_firmware	An improper authentication vulnerability in the authentication module of the Zyxel NAS326 firmware version V5.21(AAZF.14)C0 and NAS542 firmware version V5.21(ABAG.11)C0 could allow an unauthenticated attacker to obtain system information by sending a crafted URL to a vulnerable device.	2023-11-30	7.5	High
CVE-2023-40699	ibm - multiple products	IBM InfoSphere Information Server 11.7 could allow a remote attacker to cause a denial of service due to improper input validation. IBM X-Force ID: 265161.	2023-12-01	7.5	High
CVE-2023-5607	trellix - application_and_change_control	An improper limitation of a path name to a restricted directory (path traversal) vulnerability in the TACC ePO extension, for on-premises ePO servers, prior to version 8.4.0 could lead to an authorised administrator attacker executing arbitrary code through uploading a specially crafted GTI reputation file. The attacker would need the appropriate privileges to access the relevant section of the User Interface. The import logic has been updated to restrict file types and content.	2023-11-27	7.2	High
CVE-2023-6071	trellix - enterprise_security_manager	An Improper Neutralization of Special Elements used in a command vulnerability in ESM prior to version 11.6.9 allows a remote administrator to execute arbitrary code as root on the ESM. This is possible as the input isn't correctly sanitized when adding a new data source.	2023-11-30	7.2	High
CVE-2023-34055	vmware - multiple products	In Spring Boot versions 2.7.0 - 2.7.17, 3.0.0-3.0.12 and 3.1.0-3.1.5, it is possible for a user to provide specially crafted HTTP requests that may cause a denial-of-service (DoS) condition. Specifically, an application is vulnerable when all of the following are true: * the application uses Spring MVC or Spring WebFlux * org.springframework.boot:spring-boot-actuator is on the classpath	2023-11-28	6.5	Medium
CVE-2023-42504	apache - superset	An authenticated malicious user could initiate multiple concurrent requests, each requesting multiple dashboard exports, leading to a possible denial of service. This issue affects Apache Superset: before 3.0.0	2023-11-28	6.5	Medium
CVE-2023-49653	jenkins - jira	Jenkins Jira Plugin 3.11 and earlier does not set the appropriate context for credentials lookup, allowing attackers with Item/Configure permission to access and capture credentials they are not entitled to.	2023-11-29	6.5	Medium
CVE-2023-49620	apache - dolphinscheduler	Before DolphinScheduler version 3.1.0, the login user could delete UDF function in the resource center unauthorized (which almost used in sql task), with unauthorized access vulnerability (IDOR), but after version 3.1.0 we fixed this issue. We mark this cve as	2023-11-30	6.5	Medium

		moderate level because it still requires user login to operate, please upgrade to version 3.1.0 to avoid this vulnerability			
CVE-2023-42916	apple - multiple products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 17.1.2 and iPadOS 17.1.2, macOS Sonoma 14.1.2, Safari 17.1.2. Processing web content may disclose sensitive information. Apple is aware of a report that this issue may have been exploited against versions of iOS before iOS 16.7.1.	2023-11-30	6.5	Medium
CVE-2023-26024	ibm - planning_analytics_on_cloud_pak_for_data	IBM Planning Analytics on Cloud Pak for Data 4.0 could allow an attacker on a shared network to obtain sensitive information caused by insecure network communication. IBM X-Force ID: 247898.	2023-12-01	6.5	Medium
CVE-2023-35139	zyxel - zld	A cross-site scripting (XSS) vulnerability in the CGI program of the Zyxel ATP series firmware versions 5.10 through 5.37, USG FLEX series firmware versions 5.00 through 5.37, USG FLEX 50(W) series firmware versions 5.10 through 5.37, USG20(W)-VPN series firmware versions 5.10 through 5.37, and VPN series firmware versions 5.00 through 5.37, could allow an unauthenticated LAN-based attacker to store malicious scripts in a vulnerable device. A successful XSS attack could then result in the stored malicious scripts being executed to steal cookies when the user visits the specific CGI used for dumping ZTP logs.	2023-11-28	6.1	Medium
CVE-2021-36806	sophos - email_appliance	A reflected XSS vulnerability allows an open redirect when the victim clicks a malicious link to an error page on Sophos Email Appliance older than version 4.5.3.4.	2023-11-30	6.1	Medium
CVE-2023-5981	gnu - gnutls	A vulnerability was found that the response times to malformed ciphertexts in RSA-PSK ClientKeyExchange differ from response times of ciphertexts with correct PKCS#1 v1.5 padding.	2023-11-28	5.9	Medium
CVE-2023-42019	ibm - multiple products	IBM InfoSphere Information Server 11.7 could allow a remote attacker to cause a denial of service due to improper input validation. IBM X-Force ID: 265161.	2023-12-01	5.9	Medium
CVE-2023-35136	zyxel - zld	An improper input validation vulnerability in the “Quagga” package of the Zyxel ATP series firmware versions 4.32 through 5.37, USG FLEX series firmware versions 4.50 through 5.37, USG FLEX 50(W) series firmware versions 4.16 through 5.37, USG20(W)-VPN series firmware versions 4.16 through 5.37, and VPN series firmware versions 4.30 through 5.37, could allow an authenticated local attacker to access configuration files on an affected device.	2023-11-28	5.5	Medium
CVE-2023-37925	zyxel - zld	An improper privilege management vulnerability in the debug CLI command of the Zyxel ATP series firmware versions 4.32 through 5.37, USG FLEX series firmware versions 4.50 through 5.37, USG FLEX 50(W) series firmware versions 4.16 through 5.37, USG20(W)-VPN series firmware versions 4.16 through 5.37, VPN series firmware versions 4.30 through 5.37, NWA50AX firmware version 6.29(ABYW.2), WAC500 firmware version 6.65(ABVS.1), WAX300H firmware version 6.60(ACHF.1), and WBE660S firmware version 6.65(ACGG.1), could allow an authenticated local attacker to access system files on an affected device.	2023-11-28	5.5	Medium
CVE-2023-37926	zyxel - zld	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.37, USG FLEX series firmware versions 4.50 through 5.37, USG FLEX 50(W) series firmware versions 4.16 through 5.37, USG20(W)-VPN series firmware versions 4.16 through 5.37, and VPN series firmware versions 4.30 through 5.37, could allow an authenticated local attacker to cause denial-of-service (DoS) conditions by executing the CLI command to dump system logs on an affected device.	2023-11-28	5.5	Medium
CVE-2023-5650	zyxel - zld	An improper privilege management vulnerability in the ZySH of the Zyxel ATP series firmware versions 4.32 through 5.37, USG FLEX series firmware versions 4.50 through 5.37, USG FLEX 50(W) series firmware versions 4.16 through 5.37, USG20(W)-VPN series firmware versions 4.16 through 5.37, and VPN series firmware versions 4.30 through 5.37, could allow an authenticated local attacker to modify the URL of the registration page in the web GUI of an affected device.	2023-11-28	5.5	Medium
CVE-2023-5797	zyxel - zld	An improper privilege management vulnerability in the debug CLI command of the Zyxel ATP series firmware versions 4.32 through 5.37, USG FLEX series firmware versions 4.50 through 5.37, USG FLEX 50(W) series firmware versions 4.16 through 5.37, USG20(W)-VPN series firmware versions 4.16 through 5.37, VPN	2023-11-28	5.5	Medium

		series firmware versions 4.30 through 5.37, NWA50AX firmware version 6.29(ABYW.2), WAC500 firmware version 6.65(ABVS.1), WAX300H firmware version 6.60(ACHF.1), and WBE660S firmware version 6.65(ACGG.1), could allow an authenticated local attacker to access the administrator's logs on an affected device.			
CVE-2023-5960	zyxel - zld	An improper privilege management vulnerability in the hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.37 and VPN series firmware versions 4.30 through 5.37 could allow an authenticated local attacker to access the system files on an affected device.	2023-11-28	5.5	Medium
CVE-2023-42006	ibm - multiple products	IBM Administration Runtime Expert for i 7.2, 7.3, 7.4, and 7.5 could allow a local user to obtain sensitive information caused by improper authority checks. IBM X-Force ID: 265266.	2023-12-01	5.5	Medium
CVE-2023-43701	apache - superset	Improper payload validation and an improper REST API response type, made it possible for an authenticated malicious actor to store malicious code into Chart's metadata, this code could get executed if a user specifically accesses a specific deprecated API endpoint. This issue affects Apache Superset versions prior to 2.1.2. Users are recommended to upgrade to version 2.1.2, which fixes this issue.	2023-11-27	5.4	Medium
CVE-2023-49145	apache - nifi	Apache NiFi 0.7.0 through 1.23.2 include the JoltTransformJSON Processor, which provides an advanced configuration user interface that is vulnerable to DOM-based cross-site scripting. If an authenticated user, who is authorized to configure a JoltTransformJSON Processor, visits a crafted URL, then arbitrary JavaScript code can be executed within the session context of the authenticated user. Upgrading to Apache NiFi 1.24.0 or 2.0.0-M1 is the recommended mitigation.	2023-11-27	5.4	Medium
CVE-2023-42502	apache - superset	An authenticated attacker with update datasets permission could change a dataset link to an untrusted site by spoofing the HTTP Host header, users could be redirected to this site when clicking on that specific dataset. This issue affects Apache Superset versions before 3.0.0.	2023-11-28	5.4	Medium
CVE-2023-43015	ibm - multiple products	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 266064.	2023-12-01	5.4	Medium
CVE-2023-42009	ibm - multiple products	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 265504.	2023-12-01	5.4	Medium
CVE-2023-42022	ibm - multiple products	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 265938.	2023-12-01	5.4	Medium
CVE-2023-46174	ibm - multiple products	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 269506.	2023-12-01	5.4	Medium
CVE-2023-43021	ibm - multiple products	IBM InfoSphere Information Server 11.7 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 266167.	2023-12-01	5.3	Medium
CVE-2023-4397	zyxel - zld	A buffer overflow vulnerability in the Zyxel ATP series firmware version 5.37, USG FLEX series firmware version 5.37, USG FLEX 50(W) series firmware version 5.37, and USG20(W)-VPN series firmware version 5.37, could allow an authenticated local attacker with administrator privileges to cause denial-of-service (DoS) conditions by executing the CLI command with crafted strings on an affected device.	2023-11-28	4.4	Medium
CVE-2023-42501	apache - superset	Unnecessary read permissions within the Gamma role would allow authenticated users to read configured CSS templates and	2023-11-27	4.3	Medium

		annotations. This issue affects Apache Superset: before 2.1.2. Users should upgrade to version or above 2.1.2 and run `superset init` to reconstruct the Gamma role or remove `can_read` permission from the mentioned resources.			
CVE-2023-42505	apache - superset	An authenticated user with read permissions on database connections metadata could potentially access sensitive information such as the connection's username. This issue affects Apache Superset before 3.0.0.	2023-11-28	4.3	Medium
CVE-2023-6070	trellix - enterprise_security_manager	A server-side request forgery vulnerability in ESM prior to version 11.6.8 allows a low privileged authenticated user to upload arbitrary content, potentially altering configuration. This is possible through the certificate validation functionality where the API accepts uploaded content and doesn't parse for invalid data	2023-11-29	4.3	Medium
CVE-2023-49674	jenkins - neuvector_vulnerability_scanner	A missing permission check in Jenkins NeuVector Vulnerability Scanner Plugin 1.22 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified hostname and port using attacker-specified username and password.	2023-11-29	4.3	Medium
CVE-2023-43089	dell - rugged_control_center	Dell Rugged Control Center, version prior to 4.7, contains insufficient protection for the Policy folder. A local malicious standard user could potentially exploit this vulnerability to modify the content of the policy file, leading to unauthorized access to resources.	2023-12-01	3.3	Low
CVE-2023-49652	jenkins - google_compute_engine	Incorrect permission checks in Jenkins Google Compute Engine Plugin 4.550.vb_327fca_3db_11 and earlier allow attackers with global Item/Configure permission (while lacking Item/Configure permission on any particular job) to enumerate system-scoped credentials IDs of credentials stored in Jenkins and to connect to Google Cloud Platform using attacker-specified credentials IDs obtained through another method, to obtain information about existing projects. This fix has been backported to 4.3.17.1.	2023-11-29	2.7	Low

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.