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

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

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من 17 ديسمبر إلى 23 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 لـ CVSS 9.0-10.0**
- **عالي: النتيجة الأساسية لـ CVSS 7.0-8.9**
- **متوسط: النتيجة الأساسية لـ CVSS 4.0-6.9**
- **منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9**

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 17th of December to 23rd 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**

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2023-32728	zabbix - multiple products	The Zabbix Agent 2 item key smart.disk.get does not sanitize its parameters before passing them to a shell command resulting possible vulnerability for remote code execution.	2023-12-18	9.8	Critical
CVE-2023-51385	openbsd - openssh	In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.	2023-12-18	9.8	Critical
CVE-2023-41727	ivanti - avalanche	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	2023-12-19	9.8	Critical
CVE-2023-46216	ivanti - avalanche	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	2023-12-19	9.8	Critical
CVE-2023-46217	ivanti - avalanche	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	2023-12-19	9.8	Critical
CVE-2023-46220	ivanti - avalanche	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	2023-12-19	9.8	Critical
CVE-2023-46221	ivanti - avalanche	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	2023-12-19	9.8	Critical
CVE-2023-46222	ivanti - avalanche	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	2023-12-19	9.8	Critical
CVE-2023-46223	ivanti - avalanche	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	2023-12-19	9.8	Critical
CVE-2023-46224	ivanti - avalanche	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	2023-12-19	9.8	Critical
CVE-2023-46225	ivanti - avalanche	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	2023-12-19	9.8	Critical
CVE-2023-46257	ivanti - avalanche	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	2023-12-19	9.8	Critical
CVE-2023-46258	ivanti - avalanche	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	2023-12-19	9.8	Critical
CVE-2023-46259	ivanti - avalanche	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	2023-12-19	9.8	Critical
CVE-2023-46260	ivanti - avalanche	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	2023-12-19	9.8	Critical

CVE-2023-46261	ivanti - avalanche	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	2023-12-19	9.8	Critical
CVE-2023-46263	ivanti - avalanche	An unrestricted upload of file with dangerous type vulnerability exists in Avalanche versions 6.4.1 and below that could allow an attacker to achieve a remote code execution.	2023-12-19	9.8	Critical
CVE-2023-46264	ivanti - avalanche	An unrestricted upload of file with dangerous type vulnerability exists in Avalanche versions 6.4.1 and below that could allow an attacker to achieve a remove code execution.	2023-12-19	9.8	Critical
CVE-2023-46265	ivanti - avalanche	An unauthenticated could abuse a XXE vulnerability in the Smart Device Server to leak data or perform a Server-Side Request Forgery (SSRF).	2023-12-19	9.8	Critical
CVE-2023-35895	ibm - multiple products	IBM Informix JDBC Driver 4.10 and 4.50 is susceptible to remote code execution attack via JNDI injection when passing an unchecked argument to a certain API. IBM X-Force ID: 259116.	2023-12-20	9.8	Critical
CVE-2023-42017	ibm - planning_analytics	IBM Planning Analytics Local 2.0 could allow a remote attacker to upload arbitrary files, caused by the improper validation of file extensions. By sending a specially crafted HTTP request, a remote attacker could exploit this vulnerability to upload a malicious script, which could allow the attacker to execute arbitrary code on the vulnerable system. IBM X-Force ID: 265567.	2023-12-22	9.8	Critical
CVE-2021-22962	ivanti - avalanche	An attacker can send a specially crafted request which could lead to leakage of sensitive data or potentially a resource-based DoS attack.	2023-12-19	9.1	Critical
CVE-2023-46266	ivanti - avalanche	An attacker can send a specially crafted request which could lead to leakage of sensitive data or potentially a resource-based DoS attack.	2023-12-19	9.1	Critical
CVE-2023-47702	ibm - security_guardium_key_lifecycle_manager	IBM Security Guardium Key Lifecycle Manager 4.3 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view modify files on the system. IBM X-Force ID: 271196.	2023-12-20	9.1	Critical
CVE-2023-32725	zabbix - multiple products	The website configured in the URL widget will receive a session cookie when testing or executing scheduled reports. The received session cookie can then be used to access the frontend as the particular user.	2023-12-18	8.8	High
CVE-2023-49736	apache - multiple products	A where_in JINJA macro allows users to specify a quote, which combined with a carefully crafted statement would allow for SQL injection in Apache Superset.This issue affects Apache Superset: before 2.1.2, from 3.0.0 before 3.0.2. Users are recommended to upgrade to version 3.0.2, which fixes the issue.	2023-12-19	8.8	High
CVE-2023-6856	mozilla - multiple products	The WebGL `DrawElementsInstanced` method was susceptible to a heap buffer overflow when used on systems with the Mesa VM driver. This issue could allow an attacker to perform remote code execution and sandbox escape. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121.	2023-12-19	8.8	High
CVE-2023-6858	mozilla - multiple products	Firefox was susceptible to a heap buffer overflow in `nsTextFragment` due to insufficient OOM handling. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121.	2023-12-19	8.8	High
CVE-2023-6859	mozilla - multiple products	A use-after-free condition affected TLS socket creation when under memory pressure. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121.	2023-12-19	8.8	High
CVE-2023-6861	mozilla - multiple products	The `nsWindow::PickerOpen(void)` method was susceptible to a heap buffer overflow when running in headless mode. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121.	2023-12-19	8.8	High
CVE-2023-6862	mozilla - multiple products	A use-after-free was identified in the `nsDNSService::Init`. This issue appears to manifest rarely during start-up. This vulnerability affects Firefox ESR < 115.6 and Thunderbird < 115.6.	2023-12-19	8.8	High
CVE-2023-6863	mozilla - multiple products	The `ShutdownObserver()` was susceptible to potentially undefined behavior due to its reliance on a dynamic type that lacked a virtual destructor. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121.	2023-12-19	8.8	High
CVE-2023-6864	mozilla - multiple products	Memory safety bugs present in Firefox 120, Firefox ESR 115.5, and Thunderbird 115.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121.	2023-12-19	8.8	High
CVE-2023-6866	mozilla - firefox	TypedArrays can be fallible and lacked proper exception handling. This could lead to abuse in other APIs which expect TypedArrays to always succeed. This vulnerability affects Firefox < 121.	2023-12-19	8.8	High
CVE-2023-6873	mozilla - firefox	Memory safety bugs present in Firefox 120. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 121.	2023-12-19	8.8	High

CVE-2023-43826	apache - guacamole	Apache Guacamole 1.5.3 and older do not consistently ensure that values received from a VNC server will not result in integer overflow. If a user connects to a malicious or compromised VNC server, specially-crafted data could result in memory corruption, possibly allowing arbitrary code to be executed with the privileges of the running guacd process. Users are recommended to upgrade to version 1.5.4, which fixes this issue.	2023-12-19	8.8	High
CVE-2023-47706	ibm - security_guardium_key_lifecycle_manager	IBM Security Guardium Key Lifecycle Manager 4.3 could allow an authenticated user to upload files of a dangerous file type. IBM X-Force ID: 271341.	2023-12-20	8.8	High
CVE-2023-49084	cacti - cacti	Cacti is a robust performance and fault management framework and a frontend to RRDTool - a Time Series Database (TSDB). While using the detected SQL Injection and insufficient processing of the include file path, it is possible to execute arbitrary code on the server. Exploitation of the vulnerability is possible for an authorized user. The vulnerable component is the `link.php`. Impact of the vulnerability execution of arbitrary code on the server.	2023-12-21	8.8	High
CVE-2023-7024	google - chrome	Heap buffer overflow in WebRTC in Google Chrome prior to 120.0.6099.129 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-12-21	8.8	High
CVE-2023-49085	cacti - cacti	Cacti provides an operational monitoring and fault management framework. In versions 1.2.25 and prior, it is possible to execute arbitrary SQL code through the `pollers.php` script. An authorized user may be able to execute arbitrary SQL code. The vulnerable component is the `pollers.php`. Impact of the vulnerability - arbitrary SQL code execution. As of time of publication, a patch does not appear to exist.	2023-12-22	8.8	High
CVE-2023-51448	cacti - cacti	Cacti provides an operational monitoring and fault management framework. Version 1.2.25 has a Blind SQL Injection (SQLi) vulnerability within the SNMP Notification Receivers feature in the file `‘managers.php’`. An authenticated attacker with the “Settings/Utilities” permission can send a crafted HTTP GET request to the endpoint `‘/cacti/managers.php’` with an SQLi payload in the `‘selected_graphs_array’` HTTP GET parameter. As of time of publication, no patched versions exist.	2023-12-22	8.8	High
CVE-2023-41314	apache - doris	The api /api/snapshot and /api/get_log_file would allow unauthenticated access. It could allow a DoS attack or get arbitrary files from FE node. Please upgrade to 2.0.3 to fix these issues.	2023-12-18	8.2	High
CVE-2023-32726	zabbix - multiple products	The vulnerability is caused by improper check for check if RDLENGTH does not overflow the buffer in response from DNS server.	2023-12-18	8.1	High
CVE-2023-6817	linux - multiple products	A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. The function nft_pipapo_walk did not skip inactive elements during set walk which could lead double deactivations of PIPAPO (Pile Packet Policies) elements, leading to use-after-free. We recommend upgrading past commit 317eb9685095678f2c9f5a8189de698c5354316a.	2023-12-18	7.8	High
CVE-2023-6931	linux - linux_kernel	A heap out-of-bounds write vulnerability in the Linux kernel's Performance Events system component can be exploited to achieve local privilege escalation. A perf_event's read_size can overflow, leading to an heap out-of-bounds increment or write in perf_read_group(). We recommend upgrading past commit 382c27f4ed28f803b1f1473ac2d8db0afc795a1b.	2023-12-19	7.8	High
CVE-2023-6893	hikvision - intercom_broadcast_system	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252.	2023-12-17	7.5	High
CVE-2023-50271	hp - system_management_homepage	A potential security vulnerability has been identified with HP-UX	2023-12-17	7.5	High

		System Management Homepage (SMH). This vulnerability could be exploited locally or remotely to disclose information.			
CVE-2023-4320	redhat - satellite	An arithmetic overflow flaw was found in Satellite when creating a new personal access token. This flaw allows an attacker who uses this arithmetic overflow to create personal access tokens that are valid indefinitely, resulting in damage to the system's integrity.	2023-12-18	7.5	High
CVE-2023-46177	ibm - multiple products	IBM MQ Appliance 9.3 LTS and 9.3 CD could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request to view arbitrary files on the system. IBM X-Force ID: 269536.	2023-12-18	7.5	High
CVE-2023-46262	ivanti - avalanche	An unauthenticated attacked could send a specifically crafted web request causing a Server-Side Request Forgery (SSRF) in Ivanti Avalanche Remote Control server.	2023-12-19	7.5	High
CVE-2023-46803	ivanti - avalanche	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS).	2023-12-19	7.5	High
CVE-2023-46804	ivanti - avalanche	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS).	2023-12-19	7.5	High
CVE-2023-47704	ibm - security_guardium_key_lifecycle_manager	IBM Security Guardium Key Lifecycle Manager 4.3 contains plain text hard-coded credentials or other secrets in source code repository. IBM X-Force ID: 271220.	2023-12-20	7.5	High
CVE-2023-32727	zabbix - multiple products	An attacker who has the privilege to configure Zabbix items can use function icmpping() with additional malicious command inside it to execute arbitrary code on the current Zabbix server.	2023-12-18	7.2	High
CVE-2023-6932	linux - linux_kernel	A use-after-free vulnerability in the Linux kernel's ipv4: igmp component can be exploited to achieve local privilege escalation. A race condition can be exploited to cause a timer be mistakenly registered on a RCU read locked object which is freed by another thread. We recommend upgrading past commit e2b706c691905fe78468c361aaabc719d0a496f1.	2023-12-19	7	High
CVE-2023-6894	hikvision - intercom_broadcast_system	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability.	2023-12-17	6.5	Medium
CVE-2023-3628	redhat - jboss_data_grid	A flaw was found in Infinispan's REST. Bulk read endpoints do not properly evaluate user permissions for the operation. This issue could allow an authenticated user to access information outside of their intended permissions.	2023-12-18	6.5	Medium
CVE-2023-3629	redhat - data_grid	A flaw was found in Infinispan's REST, Cache retrieval endpoints do not properly evaluate the necessary admin permissions for the operation. This issue could allow an authenticated user to access information outside of their intended permissions.	2023-12-18	6.5	Medium
CVE-2023-5236	redhat - data_grid	A flaw was found in Infinispan, which does not detect circular object references when unmarshalling. An authenticated attacker with sufficient permissions could insert a maliciously constructed object into the cache and use it to cause out of memory errors and achieve a denial of service.	2023-12-18	6.5	Medium
CVE-2023-46104	apache - multiple products	Uncontrolled resource consumption can be triggered by authenticated attacker that uploads a malicious ZIP to import database, dashboards or datasets. This vulnerability exists in Apache Superset versions up to and including 2.1.2 and versions 3.0.0, 3.0.1.	2023-12-19	6.5	Medium
CVE-2023-49734	apache - multiple products	An authenticated Gamma user has the ability to create a dashboard and add charts to it, this user would automatically become one of the owners of the charts allowing him to incorrectly have write permissions to these charts.This issue affects Apache Superset: before 2.1.2, from 3.0.0 before 3.0.2. Users are recommended to upgrade to version 3.0.2 or 2.1.3, which fixes the issue.	2023-12-19	6.5	Medium
CVE-2023-6860	mozilla - multiple products	The `VideoBridge` allowed any content process to use textures produced by remote decoders. This could be abused to escape the sandbox. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121.	2023-12-19	6.5	Medium
CVE-2023-6865	mozilla - multiple products	`EncryptingOutputStream` was susceptible to exposing uninitialized data. This issue could only be abused in order to write data to a local disk which may have implications for private browsing mode. This vulnerability affects Firefox ESR < 115.6 and Firefox < 121.	2023-12-19	6.5	Medium

CVE-2023-6869	mozilla - firefox	A `<dialog>` element could have been manipulated to paint content outside of a sandboxed iframe. This could allow untrusted content to display under the guise of trusted content. This vulnerability affects Firefox < 121.	2023-12-19	6.5	Medium
CVE-2023-6872	mozilla - firefox	Browser tab titles were being leaked by GNOME to system logs. This could potentially expose the browsing habits of users running in a private tab. This vulnerability affects Firefox < 121.	2023-12-19	6.5	Medium
CVE-2023-47146	ibm - multiple products	IBM Qradar SIEM 7.5 could allow a privileged user to obtain sensitive domain information due to data being misidentified. IBM X-Force ID: 270372.	2023-12-19	6.5	Medium
CVE-2023-47161	ibm - multiple products	IBM UrbanCode Deploy (UCD) 7.1 through 7.1.2.14, 7.2 through 7.2.3.7, and 7.3 through 7.3.2.2 may mishandle input validation of an uploaded archive file leading to a denial of service due to resource exhaustion. IBM X-Force ID: 270799.	2023-12-20	6.5	Medium
CVE-2023-49920	apache - airflow	Apache Airflow, version 2.7.0 through 2.7.3, has a vulnerability that allows an attacker to trigger a DAG in a GET request without CSRF validation. As a result, it was possible for a malicious website opened in the same browser - by the user who also had Airflow UI opened - to trigger the execution of DAGs without the user's consent. Users are advised to upgrade to version 2.8.0 or later which is not affected	2023-12-21	6.5	Medium
CVE-2023-50783	apache - airflow	Apache Airflow, versions before 2.8.0, is affected by a vulnerability that allows an authenticated user without the variable edit permission, to update a variable. This flaw compromises the integrity of variable management, potentially leading to unauthorized data modification. Users are recommended to upgrade to 2.8.0, which fixes this issue	2023-12-21	6.5	Medium
CVE-2023-5115	redhat - multiple products	An absolute path traversal attack exists in the Ansible automation platform. This flaw allows an attacker to craft a malicious Ansible role and make the victim execute the role. A symlink can be used to overwrite a file outside of the extraction path.	2023-12-18	6.3	Medium
CVE-2023-6927	redhat - keycloak	A flaw was found in Keycloak. This issue may allow an attacker to steal authorization codes or tokens from clients using a wildcard in the JARM response mode "form_post.jwt" which could be used to bypass the security patch implemented to address CVE-2023-6134.	2023-12-18	6.1	Medium
CVE-2023-6867	mozilla - multiple products	The timing of a button click causing a popup to disappear was approximately the same length as the anti-clickjacking delay on permission prompts. It was possible to use this fact to surprise users by luring them to click where the permission grant button would be about to appear. This vulnerability affects Firefox ESR < 115.6 and Firefox < 121.	2023-12-19	6.1	Medium
CVE-2023-50569	cacti - cacti	Reflected Cross Site Scripting (XSS) vulnerability in Cacti v1.2.25, allows remote attackers to escalate privileges when uploading an xml template file via templates_import.php.	2023-12-22	6.1	Medium
CVE-2023-50250	cacti - cacti	Cacti is an open source operational monitoring and fault management framework. A reflection cross-site scripting vulnerability was discovered in version 1.2.25. Attackers can exploit this vulnerability to perform actions on behalf of other users. The vulnerability is found in `templates_import.php.` When uploading an xml template file, if the XML file does not pass the check, the server will give a JavaScript pop-up prompt, which contains unfiltered xml template file name, resulting in XSS. An attacker exploiting this vulnerability could execute actions on behalf of other users. This ability to impersonate users could lead to unauthorized changes to settings. As of time of publication, no patched versions are available.	2023-12-22	6.1	Medium
CVE-2023-48795	openbsd - openssh	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144,	2023-12-18	5.9	Medium

		CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.			
CVE-2023-51384	openbsd - openssh	In ssh-agent in OpenSSH before 9.6, certain destination constraints can be incompletely applied. When destination constraints are specified during addition of PKCS#11-hosted private keys, these constraints are only applied to the first key, even if a PKCS#11 token returns multiple keys.	2023-12-18	5.5	Medium
CVE-2023-45172	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 AIX windows to cause a denial of service. IBM X-Force ID: 267970.	2023-12-19	5.5	Medium
CVE-2023-42012	ibm - multiple products	An IBM UrbanCode Deploy Agent 7.2 through 7.2.3.7, and 7.3 through 7.3.2.2 installed as a Windows service in a non-standard location could be subject to a denial of service attack by local accounts. IBM X-Force ID: 265509.	2023-12-20	5.5	Medium
CVE-2023-45165	ibm - multiple products	IBM AIX 7.2 and 7.3 could allow a non-privileged local user to exploit a vulnerability in the AIX SMB client to cause a denial of service. IBM X-Force ID: 267963.	2023-12-22	5.5	Medium
CVE-2023-47707	ibm - security_guardium_key_lifecycle_manager	IBM Security Guardium Key Lifecycle Manager 4.3 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: 271522.	2023-12-20	5.4	Medium
CVE-2023-51457	adobe - experience_manager	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	2023-12-20	5.4	Medium
CVE-2023-51458	adobe - experience_manager	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	2023-12-20	5.4	Medium
CVE-2023-51459	adobe - experience_manager	Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-12-20	5.4	Medium
CVE-2023-51460	adobe - experience_manager	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	2023-12-20	5.4	Medium
CVE-2023-51461	adobe - experience_manager	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	2023-12-20	5.4	Medium
CVE-2023-51462	adobe - multiple products	Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-12-20	5.4	Medium
CVE-2023-47265	apache - airflow	Apache Airflow, versions 2.6.0 through 2.7.3 has a stored XSS vulnerability that allows a DAG author to add an unbounded and not-sanitized javascript in the parameter description field of the DAG. This Javascript can be executed on the client side of any of the user who looks at the tasks in the browser sandbox. While this issue does not allow to exit the browser sandbox or manipulation of the server-side data - more than the DAG author already has, it allows to modify what the user looking at the DAG details sees in the browser - which opens up all kinds of possibilities of misleading other users. Users of Apache Airflow are recommended to upgrade to version 2.8.0 or newer to mitigate the risk associated with this vulnerability	2023-12-21	5.4	Medium

CVE-2023-49086	cacti - cacti	Cacti is a robust performance and fault management framework and a frontend to RRDTool - a Time Series Database (TSDB). Bypassing an earlier fix (CVE-2023-39360) that leads to a DOM XSS attack. Exploitation of the vulnerability is possible for an authorized user. The vulnerable component is the `graphs_new.php`. Impact of the vulnerability - execution of arbitrary javascript code in the attacked user's browser. This issue has been patched in version 1.2.26.	2023-12-22	5.4	Medium
CVE-2023-28053	dell - emc_networker	Dell NetWorker Virtual Edition versions 19.8 and below contain the use of deprecated cryptographic algorithms in the SSH component. A remote unauthenticated attacker could potentially exploit this vulnerability leading to some information disclosure.	2023-12-18	5.3	Medium
CVE-2023-47741	ibm - multiple products	IBM i 7.3, 7.4, 7.5, IBM i Db2 Mirror for i 7.4 and 7.5 web browser clients may leave clear-text passwords in browser memory that can be viewed using common browser tools before the memory is garbage collected. A malicious actor with access to the victim's PC could exploit this vulnerability to gain access to the IBM i operating system. IBM X-Force ID: 272532.	2023-12-18	5.3	Medium
CVE-2023-6857	mozilla - multiple products	When resolving a symlink, a race may occur where the buffer passed to `readlink` may actually be smaller than necessary. *This bug only affects Firefox on Unix-based operating systems (Android, Linux, MacOS). Windows is unaffected.* This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121.	2023-12-19	5.3	Medium
CVE-2023-42013	ibm - multiple products	IBM UrbanCode Deploy (UCD) 7.1 through 7.1.2.14, 7.2 through 7.2.3.7, and 7.3 through 7.3.2.2 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: 265510.	2023-12-20	5.3	Medium
CVE-2023-47703	ibm - security_guardium_key_lifecycle_manager	IBM Security Guardium Key Lifecycle Manager 4.3 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: 271197.	2023-12-20	5.3	Medium
CVE-2023-40691	ibm - multiple products	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 may reveal sensitive information contained in application configuration to developer and administrator users. IBM X-Force ID: 264805.	2023-12-18	4.9	Medium
CVE-2023-6911	wso2 - multiple products	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console.	2023-12-18	4.8	Medium
CVE-2023-49088	cacti - cacti	Cacti is an open source operational monitoring and fault management framework. The fix applied for CVE-2023-39515 in version 1.2.25 is incomplete as it enables an adversary to have a victim browser execute malicious code when a victim user hovers their mouse over the malicious data source path in `data_debug.php`. To perform the cross-site scripting attack, the adversary needs to be an authorized cacti user with the following permissions: `General Administration>Sites/Devices/Data`. The victim of this attack could be any account with permissions to view `http://<HOST>/cacti/data_debug.php`. As of time of publication, no complete fix has been included in Cacti.	2023-12-22	4.8	Medium
CVE-2023-42015	ibm - multiple products	IBM UrbanCode Deploy (UCD) 7.1 through 7.1.2.14, 7.2 through 7.2.3.7, and 7.3 through 7.3.2.2 is vulnerable to HTML injection. This vulnerability may allow a user to embed arbitrary HTML tags in the Web UI potentially leading to sensitive information disclosure. IBM X-Force ID: 265512.	2023-12-19	4.3	Medium
CVE-2023-50761	mozilla - thunderbird	The signature of a digitally signed S/MIME email message may optionally specify the signature creation date and time. If present, Thunderbird did not compare the signature creation date with the message date and time, and displayed a valid signature despite a date or time mismatch. This could be used to give recipients the impression that a message was sent at a different date or time. This vulnerability affects Thunderbird < 115.6.	2023-12-19	4.3	Medium
CVE-2023-50762	mozilla - thunderbird	When processing a PGP/MIME payload that contains digitally signed text, the first paragraph of the text was never shown to the user. This is because the text was interpreted as a MIME message and the first paragraph was always treated as an email header section. A digitally signed text from a different context, such as a signed GIT commit, could be used to spoof an email message. This vulnerability affects Thunderbird < 115.6.	2023-12-19	4.3	Medium

CVE-2023-6135	mozilla - firefox	Multiple NSS NIST curves were susceptible to a side-channel attack known as "Minerva". This attack could potentially allow an attacker to recover the private key. This vulnerability affects Firefox < 121.	2023-12-19	4.3	Medium
CVE-2023-6868	mozilla - firefox	In some instances, the user-agent would allow push requests which lacked a valid VAPID even though the push manager subscription defined one. This could allow empty messages to be sent from unauthorized parties. *This bug only affects Firefox on Android.* This vulnerability affects Firefox < 121.	2023-12-19	4.3	Medium
CVE-2023-6870	mozilla - multiple products	Applications which spawn a Toast notification in a background thread may have obscured fullscreen notifications displayed by Firefox. *This issue only affects Android versions of Firefox and Firefox Focus.* This vulnerability affects Firefox < 121.	2023-12-19	4.3	Medium
CVE-2023-6871	mozilla - firefox	Under certain conditions, Firefox did not display a warning when a user attempted to navigate to a new protocol handler. This vulnerability affects Firefox < 121.	2023-12-19	4.3	Medium
CVE-2023-47705	ibm - security_guardium_key_lifecycle_manager	IBM Security Guardium Key Lifecycle Manager 4.3 could allow an authenticated user to manipulate username data due to improper input validation. IBM X-Force ID: 271228.	2023-12-20	4.3	Medium
CVE-2023-48291	apache - airflow	Apache Airflow, in versions prior to 2.8.0, contains a security vulnerability that allows an authenticated user with limited access to some DAGs, to craft a request that could give the user write access to various DAG resources for DAGs that the user had no access to, thus, enabling the user to clear DAGs they shouldn't. This is a missing fix for CVE-2023-42792 in Apache Airflow 2.7.2 Users of Apache Airflow are strongly advised to upgrade to version 2.8.0 or newer to mitigate the risk associated with this vulnerability.	2023-12-21	4.3	Medium
CVE-2023-5056	redhat - service_interconnect	A flaw was found in the Skupper operator, which may permit a certain configuration to create a service account that would allow an authenticated attacker in the adjacent cluster to view deployments in all namespaces in the cluster. This issue permits unauthorized viewing of information outside of the user's purview.	2023-12-18	4.1	Medium
CVE-2023-5384	redhat - data_grid	A flaw was found in Infinispan. When serializing the configuration for a cache to XML/JSON/YAML, which contains credentials (JDBC store with connection pooling, remote store), the credentials are returned in clear text as part of the configuration.	2023-12-18	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.