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.

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 24th of November to 30th of November. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

- **Critical: CVSS base score of 9.0-10.0**
- **High: CVSS base score of 7.0-8.9**
- **Medium: CVSS base score 4.0-6.9**
- **Low: CVSS base score 0.0-3.9**

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

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من ٢٤ نوفمبر إلى ٣٠ نوفمبر. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score
CVE-2024-42327	zabbix - Zabbix	A non-admin user account on the Zabbix frontend with the default User role, or with any other role that gives API access can exploit this vulnerability. An SQLi exists in the CUser class in the addRelatedObjects function, this function is being called from the CUser.get function which is available for every user who has API access.	2024-11-27	9.9
CVE-2024-11236	php - multiple products	In PHP versions 8.1.* before 8.1.31, 8.2.* before 8.2.26, 8.3.* before 8.3.14, uncontrolled long string inputs to ldap_escape() function on 32-bit systems can cause an integer overflow, resulting in an out-of-bounds write.	2024-11-24	9.8
CVE-2024-53909	veritas - enterprise_vault	An issue was discovered in the server in Veritas Enterprise Vault before 15.2, ZDI-CAN-24334. It allows remote attackers to execute arbitrary code because untrusted data, received on a .NET Remoting TCP port, is deserialized.	2024-11-24	9.8
CVE-2024-53910	veritas - enterprise_vault	An issue was discovered in the server in Veritas Enterprise Vault before 15.2, ZDI-CAN-24336. It allows remote attackers to execute arbitrary code because untrusted data, received on a .NET Remoting TCP port, is deserialized.	2024-11-24	9.8
CVE-2024-53911	veritas - enterprise_vault	An issue was discovered in the server in Veritas Enterprise Vault before 15.2, ZDI-CAN-24339. It allows remote attackers to execute arbitrary code because untrusted data, received on a .NET Remoting TCP port, is deserialized.	2024-11-24	9.8
CVE-2024-53912	veritas - enterprise_vault	An issue was discovered in the server in Veritas Enterprise Vault before 15.2, ZDI-CAN-24341. It allows remote attackers to execute arbitrary code because untrusted data, received on a .NET Remoting TCP port, is deserialized.	2024-11-24	9.8
CVE-2024-53913	veritas - enterprise_vault	An issue was discovered in the server in Veritas Enterprise Vault before 15.2, ZDI-CAN-24343. It allows remote attackers to execute arbitrary code because untrusted data, received on a .NET Remoting TCP port, is deserialized.	2024-11-24	9.8
CVE-2024-53914	veritas - enterprise_vault	An issue was discovered in the server in Veritas Enterprise Vault before 15.2, ZDI-CAN-24344. It allows remote attackers to execute arbitrary code because untrusted data, received on a .NET Remoting TCP port, is deserialized.	2024-11-24	9.8
CVE-2024-53915	veritas - enterprise_vault	An issue was discovered in the server in Veritas Enterprise Vault before 15.2, ZDI-CAN-24405. It allows remote attackers to execute arbitrary code because untrusted data, received on a .NET Remoting TCP port, is deserialized.	2024-11-24	9.8
CVE-2024-11693	mozilla - multiple products	The executable file warning was not presented when downloading .library-ms files. *Note: This issue only affected Windows operating systems. Other operating systems are unaffected.* This vulnerability affects Firefox < 133, Firefox ESR < 128.5, Thunderbird < 133, and Thunderbird < 128.5.	2024-11-26	9.8
CVE-2024-11698	mozilla - multiple products	A flaw in handling fullscreen transitions may have inadvertently caused the application to become stuck in fullscreen mode when a modal dialog was opened during the transition. This issue left users unable to exit fullscreen mode using standard actions like pressing "Esc" or accessing right-click menus, resulting in a disrupted browsing experience until the browser is restarted. *This bug only affects the application when running on macOS. Other operating systems are unaffected.* This vulnerability affects Firefox < 133, Firefox ESR < 128.5, Thunderbird < 133, and Thunderbird < 128.5.	2024-11-26	9.8
CVE-2024-11704	mozilla - multiple products	A double-free issue could have occurred in \`sec_pkcs7_decoder_start_decrypt()\` when handling an error path. Under specific conditions, the same symmetric key could have been freed twice, potentially leading to memory corruption. This vulnerability affects Firefox < 133 and Thunderbird < 133.	2024-11-26	9.8

CVE-2024-53676	hewlett packard enterprise (hpe) - HPE Insight Remote Support	A directory traversal vulnerability in Hewlett Packard Enterprise Insight Remote Support may allow remote code execution.	2024-11-27	9.8
CVE-2024-52338	apache software foundation - Apache Arrow R package	Deserialization of untrusted data in IPC and Parquet readers in the Apache Arrow R package versions 4.0.0 through 16.1.0 allows arbitrary code execution. An application is vulnerable if it reads Arrow IPC, Feather or Parquet data from untrusted sources (for example, user-supplied input files). This vulnerability only affects the arrow R package, not other Apache Arrow implementations or bindings unless those bindings are specifically used via the R package (for example, an R application that embeds a Python interpreter and uses PyArrow to read files from untrusted sources is still vulnerable if the arrow R package is an affected version). It is recommended that users of the arrow R package upgrade to 17.0.0 or later. Similarly, it is recommended that downstream libraries upgrade their dependency requirements to arrow 17.0.0 or later. If using an affected version of the package, untrusted data can read into a Table and its internal to_data_frame() method can be used as a workaround (e.g., read_parquet(..., as_data_frame = FALSE)$to_data_frame()). This issue affects the Apache Arrow R package: from 4.0.0 through 16.1.0. Users are recommended to upgrade to version 17.0.0, which fixes the issue.	2024-11-28	9.8
CVE-2024-11482	trellix - Trellix Enterprise Security Manager (ESM)	A vulnerability in ESM 11.6.10 allows unauthenticated access to the internal Snowservice API and enables remote code execution through command injection, executed as the root user.	2024-11-29	9.8
CVE-2024-49803	ibm - Security Verify Access	IBM Security Verify Access Appliance 10.0.0 through 10.0.8 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request.	2024-11-29	9.8
CVE-2024-49805	ibm - Security Verify Access	IBM Security Verify Access Appliance 10.0.0 through 10.0.8 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data.	2024-11-29	9.4
CVE-2024-49806	ibm - Security Verify Access	IBM Security Verify Access Appliance 10.0.0 through 10.0.8 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data.	2024-11-29	9.4
CVE-2024-49038	microsoft - Microsoft Copilot Studio	Improper neutralization of input during web page generation ('Cross-site Scripting') in Copilot Studio by an unauthorized attacker leads to elevation of privilege over a network.	2024-11-26	9.3
CVE-2024-11705	mozilla - multiple products	\`NSC_DeriveKey\` inadvertently assumed that the \`phKey\` parameter is always non-NULL. When it was passed as NULL, a segmentation fault (SEGV) occurred, leading to crashes. This behavior conflicted with the PKCS#11 v3.0 specification, which allows \`phKey\` to be NULL for certain mechanisms. This vulnerability affects Firefox < 133 and Thunderbird < 133.	2024-11-26	9.1
CVE-2024-42330	zabbix - Zabbix	The HttpRequest object allows to get the HTTP headers from the server's response after sending the request. The problem is that the returned strings are created directly from the data returned by the server and are not correctly encoded for JavaScript. This allows to create internal strings that can be used to access hidden properties of objects.	2024-11-27	9.1
CVE-2024-11691	mozilla - multiple products	Certain WebGL operations on Apple silicon M series devices could have lead to an out-of-bounds write and memory corruption due to a flaw in Apple's GPU driver. *This bug only affected the application on Apple M series hardware. Other platforms were unaffected.* This vulnerability affects Firefox < 133, Firefox ESR < 128.5, Firefox ESR < 115.18, Thunderbird < 133, and Thunderbird < 128.5.	2024-11-26	8.8
CVE-2024-11697	mozilla - multiple products	When handling keypress events, an attacker may have been able to trick a user into bypassing the "Open Executable File?" confirmation dialog. This could have led to malicious code execution. This vulnerability affects Firefox < 133, Firefox ESR < 128.5, Thunderbird < 133, and Thunderbird < 128.5.	2024-11-26	8.8
CVE-2024-11699	mozilla - multiple products	Memory safety bugs present in Firefox 132, Firefox ESR 128.4, and Thunderbird 128.4. 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 < 133, Firefox ESR < 128.5, Thunderbird < 133, and Thunderbird < 128.5.	2024-11-26	8.8
CVE-2024-7025	google - Chrome	Integer overflow in Layout in Google Chrome prior to 129.0.6668.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-11-27	8.8
CVE-2024-36466	zabbix - Zabbix	A bug in the code allows an attacker to sign a forged zbx_session cookie, which then allows them to sign in with admin permissions.	2024-11-28	8.8
CVE-2024-49035	microsoft - Microsoft Partner Center	An improper access control vulnerability in Partner.Microsoft.com allows an a unauthenticated attacker to elevate privileges over a network.	2024-11-26	8.7
CVE-2024-52899	ibm - Data Virtualization Manager for z/OS	IBM Data Virtualization Manager for z/OS 1.1 and 1.2 could allow an authenticated user to inject malicious JDBC URL parameters and execute code on the server.	2024-11-26	8.5
CVE-2023-0163	mozilla - Convict	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') vulnerability in Mozilla Convict. This allows an attacker to inject attributes that are used in other components, or to override existing attributes with ones that have incompatible type, which may lead to a crash. The main use case of Convict is for handling server-side configurations written by the admins owning the servers, and not random users. So it's unlikely that an admin would deliberately sabotage their own server. Still, a situation can happen where an admin not knowledgeable about JavaScript could be tricked by an attacker into writing the malicious JavaScript code into some config files. This issue affects Convict: before 6.2.4.	2024-11-26	8.4
CVE-2017-13316	google - Android	In checkPermissions of RecognitionService.java, there is a possible permissions bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-27	8.4
CVE-2017-13323	google - Android	In String16 of String16.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege in an unprivileged process with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-27	8.4
CVE-2024-49052	microsoft - Microsoft Azure Functions	Missing authentication for critical function in Microsoft Azure PolicyWatch allows an unauthorized attacker to elevate privileges over a network.	2024-11-26	8.2

CVE-2024-11481	trellix - Trellix Enterprise Security Manager (ESM)	A vulnerability in ESM 11.6.10 allows unauthenticated access to the internal Snowservice API. This leads to improper handling of path traversal, insecure forwarding to an AJP backend without adequate validation, and lack of authentication for accessing internal API endpoints.	2024-11-29	8.2
CVE-2024-11700	mozilla - multiple products	Malicious websites may have been able to perform user intent confirmation through tapjacking. This could have led to users unknowingly approving the launch of external applications, potentially exposing them to underlying vulnerabilities. This vulnerability affects Firefox < 133 and Thunderbird < 133.	2024-11-26	8.1
CVE-2024-53673	hewlett packard enterprise (hpe) - Insight Remote Support	A java deserialization vulnerability in HPE Remote Insight Support may allow an unauthenticated attacker to execute code.	2024-11-26	8.1
CVE-2024-52323	manageengine - Analytics Plus	Zohocorp ManageEngine Analytics Plus versions below 6100 are vulnerable to authenticated sensitive data exposure which allows the users to retrieve sensitive tokens associated to the org-admin account.	2024-11-27	8.1
CVE-2023-1521	mozilla - sccache	On Linux the sccache client can execute arbitrary code with the privileges of a local sccache server, by preloading the code in a shared library passed to LD_PRELOAD. If the server is run as root (which is the default when installing the snap package https://snapcraft.io/sccache), this means a user running the sccache client can get root privileges.	2024-11-26	7.8
CVE-2024-38830	vmware - VMware Aria Operations	VMware Aria Operations contains a local privilege escalation vulnerability. A malicious actor with local administrative privileges may trigger this vulnerability to escalate privileges to root user on the appliance running VMware Aria Operations.	2024-11-26	7.8
CVE-2024-38831	vmware - VMware Aria Operations	VMware Aria Operations contains a local privilege escalation vulnerability. A malicious actor with local administrative privileges can insert malicious commands into the properties file to escalate privileges to a root user on the appliance running VMware Aria Operations.	2024-11-26	7.8
CVE-2024-52336	red hat - multiple products	A script injection vulnerability was identified in the Tuned package. The `instance_create()` D-Bus function can be called by locally logged-in users without authentication. This flaw allows a local non-privileged user to execute a D-Bus call with `script_pre` or `script_post` options that permit arbitrary scripts with their absolute paths to be passed. These user or attacker-controlled executable scripts or programs could then be executed by Tuned with root privileges that could allow attackers to local privilege escalation.	2024-11-26	7.8
CVE-2018-9374	google - Android	In installPackageLI of PackageManagerService.java, there is a possible permissions bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.	2024-11-28	7.8
CVE-2024-49804	ibm - Security Verify Access	IBM Security Verify Access Appliance 10.0.0 through 10.0.8 could allow a locally authenticated non-administrative user to escalate their privileges due to unnecessary permissions used to perform certain tasks.	2024-11-29	7.8
CVE-2024-49595	dell - Wyse Management Suite	Dell Wyse Management Suite, version WMS 4.4 and before, contain an Authentication Bypass by Capture-replay vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Denial of service.	2024-11-26	7.6
CVE-2024-49597	dell - Wyse Management Suite	Dell Wyse Management Suite, versions WMS 4.4 and prior, contain an Improper Restriction of Excessive Authentication Attempts vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Protection mechanism bypass.	2024-11-26	7.6
CVE-2024-49053	microsoft - multiple products	Microsoft Dynamics 365 Sales Spoofing Vulnerability	2024-11-26	7.6
CVE-2024-49353	ibm - Watson Speech Services Cartridge for IBM Cloud Pak for Data	IBM Watson Speech Services Cartridge for IBM Cloud Pak for Data 4.0.0 through 5.0.2 does not properly check inputs to resources that are used concurrently, which might lead to unexpected states, possibly resulting in a crash.	2024-11-26	7.5
CVE-2024-51569	apache software foundation - Apache NimBLE	Out-of-bounds Read vulnerability in Apache NimBLE. Missing proper validation of HCI Number Of Completed Packets could lead to out-of-bound access when parsing HCI event and invalid read from HCI transport memory. This issue requires broken or bogus Bluetooth controller and thus severity is considered low. This issue affects Apache NimBLE: through 1.7.0. Users are recommended to upgrade to version 1.8.0, which fixes the issue.	2024-11-26	7.5
CVE-2024-11702	mozilla - multiple products	Copying sensitive information from Private Browsing tabs on Android, such as passwords, may have inadvertently stored data in the cloud-based clipboard history if enabled. This vulnerability affects Firefox < 133 and Thunderbird < 133.	2024-11-26	7.5
CVE-2024-36467	zabbix - Zabbix	An authenticated user with API access (e.g.: user with default User role), more specifically a user with access to the user.update API endpoint is enough to be able to add themselves to any group (e.g.: Zabbix Administrators), except to groups that are disabled or having restricted GUI access.	2024-11-27	7.5
CVE-2024-11667	zyxel - zld	A directory traversal vulnerability in the web management interface of Zyxel ATP series firmware versions V5.00 through V5.38, USG FLEX series firmware versions V5.00 through V5.38, USG FLEX 50(W) series firmware versions V5.10 through V5.38, and USG20(W)-VPN series firmware versions V5.10 through V5.38 could allow an attacker to download or upload files via a crafted URL.	2024-11-27	7.5
CVE-2017-13319	google - Android	In pvmp3_get_main_data_size of pvmp3_get_main_data_size.cpp, there is a possible buffer overread due to a missing bounds check. This could lead to remote information disclosure of global static variables with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-27	7.5
CVE-2024-8676	red hat - multiple products	A vulnerability was found in CRI-O, where it can be requested to take a checkpoint archive of a container and later be asked to restore it. When it does that restoration, it attempts to restore the mounts from the restore archive instead of the pod request. As a result, the validations run on the pod spec, verifying that the pod has access to the mounts it specifies are not applicable to a restored container. This flaw allows a malicious user to trick CRI-O into restoring a pod that doesn't have access to host mounts. The user needs access to the kubelet or cri-o socket to call the restore endpoint and trigger the restore.	2024-11-26	7.4
CVE-2024-11622	hewlett packard enterprise (hpe) - HPE Insight Remote Support	An XML external entity injection (XXE) vulnerability in HPE Insight Remote Support may allow remote users to disclose information in certain cases.	2024-11-26	7.3

CVE-2024-53674	hewlett packard enterprise (hpe) - HPE Insight Remote Support	An XML external entity injection (XXE) vulnerability in HPE Insight Remote Support may allow remote users to disclose information in certain cases.	2024-11-26	7.3
CVE-2024-53675	hewlett packard enterprise (hpe) - HPE Insight Remote Support	An XML external entity injection (XXE) vulnerability in HPE Insight Remote Support may allow remote users to disclose information in certain cases.	2024-11-26	7.3
CVE-2024-38832	vmware - VMware Aria Operations	VMware Aria Operations contains a stored cross-site scripting vulnerability. A malicious actor with editing access to views may be able to inject malicious script leading to stored cross-site scripting in the product VMware Aria Operations.	2024-11-26	7.1
CVE-2024-38833	vmware - VMware Aria Operations	VMware Aria Operations contains a stored cross-site scripting vulnerability. A malicious actor with editing access to email templates might inject malicious script leading to stored cross-site scripting in the product VMware Aria Operations.	2024-11-26	6.8
CVE-2024-38834	vmware - VMware Aria Operations	VMware Aria Operations contains a stored cross-site scripting vulnerability. A malicious actor with editing access to cloud provider might be able to inject malicious script leading to stored cross-site scripting in the product VMware Aria Operations.	2024-11-26	6.5
CVE-2024-11706	mozilla - multiple products	A null pointer dereference may have inadvertently occurred in `pk12util`, and specifically in the `SEC_ASN1DecodeItem_Util` function, when handling malformed or improperly formatted input files. This vulnerability affects Firefox < 133 and Thunderbird < 133.	2024-11-26	6.5
CVE-2024-11708	mozilla - multiple products	Missing thread synchronization primitives could have led to a data race on members of the PlaybackParams structure. This vulnerability affects Firefox < 133 and Thunderbird < 133.	2024-11-26	6.5
CVE-2024-36463	zabbix - Zabbix	The implementation of atob in "Zabbix JS" allows to create a string with arbitrary content and use it to access internal properties of objects.	2024-11-26	6.5
CVE-2017-13320	google - Android	In impeg2d_bit_stream_flush() of libmpeg2dec there is a possible OOB read due to a missing bounds check. This could lead to Remote DoS with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-27	6.5
CVE-2018-9349	google - Android	In mv_err_cost of mcomp.c there is a possible out of bounds read due to missing bounds check. This could lead to denial of service with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-27	6.5
CVE-2018-9350	google - Android	In ih264d_assign_pic_num of ih264d_utils.c there is a possible out of bound read due to missing bounds check. This could lead to a denial of service with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-27	6.5
CVE-2018-9351	google - Android	In ih264e_fmt_conv_420p_to_420sp of ih264e_fmt_conv.c there is a possible out of bound read due to missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-27	6.5
CVE-2018-9352	google - Android	In ihevcd_allocate_dynamic_bufs of ihevcd_api.c there is a possible resource exhaustion due to integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-27	6.5
CVE-2018-9353	google - Android	In ihevcd_parse_slice_data of ihevcd_parse_slice.c there is a possible heap buffer out of bound read due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-27	6.5
CVE-2018-9354	google - Android	In VideoFrameScheduler.cpp of VideoFrameScheduler::PLL::fit, there is a possible remote denial of service due to divide by 0. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-27	6.5
CVE-2024-21703	atlassian - multiple products	This Medium severity Security Misconfiguration vulnerability was introduced in version 8.8.1 of Confluence Data Center and Server for Windows installations. This Security Misconfiguration vulnerability, with a CVSS Score of 6.4 allows an authenticated attacker of the Windows host to read sensitive information about the Confluence Data Center configuration which has high impact to confidentiality, high impact to integrity, high impact to availability, and no user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to the latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release greater than or equal to 7.19.18 * Confluence Data Center and Server 8.5: Upgrade to a release greater than or equal to 8.5.5 * Confluence Data Center and Server 8.7: Upgrade to a release greater than or equal to 8.7.2 * Confluence Data Center and Server 8.8: Upgrade to a release greater than or equal to 8.8.0 See the release notes (https://confluence.atlassian.com/conf88/confluence-release-notes-1354501008.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives). This vulnerability was reported via our Atlassian Bug Bounty Program by Chris Elliot.	2024-11-27	6.4
CVE-2024-47248	apache software foundation - Apache NimBLE	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in Apache NimBLE. Specially crafted MESH message could result in memory corruption when non-default build configuration is used. This issue affects Apache NimBLE: through 1.7.0. Users are recommended to upgrade to version 1.8.0, which fixes the issue.	2024-11-26	6.3
CVE-2017-13321	google - Android	In SensorService::isDataInjectionEnabled of frameworks/native/services/sensorservice/SensorService.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-27	6.2
CVE-2018-9377	google - Android	In BnAudioPolicyService::onTransact of IAudioPolicyService.cpp, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-28	6.2
CVE-2023-45181	ibm - Jazz Foundation	IBM Jazz Foundation 7.0.2 and below are 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.	2024-11-25	6.1
CVE-2023-2142	mozilla - Nunjucks	In Nunjucks versions prior to version 3.2.4, it was possible to bypass the restrictions which are provided by the autoescape functionality. If there are two user-controlled parameters on the same line used in the views, it was possible to inject cross site scripting payloads using the backslash \ character.	2024-11-26	6.1

CVE-2024-11694	mozilla - multiple products	Enhanced Tracking Protection's Strict mode may have inadvertently allowed a CSP `frame-src` bypass and DOM-based XSS through the Google SafeFrame shim in the Web Compatibility extension. This issue could have exposed users to malicious frames masquerading as legitimate content. This vulnerability affects Firefox < 133, Firefox ESR < 128.5, Firefox ESR < 115.18, Thunderbird < 133, and Thunderbird < 128.5.	2024-11-26	6.1
CVE-2024-10451	red hat - multiple products	A flaw was found in Keycloak. This issue occurs because sensitive runtime values, such as passwords, may be captured during the Keycloak build process and embedded as default values in bytecode, leading to unintended information disclosure. In Keycloak 26, sensitive data specified directly in environment variables during the build process is also stored as a default values, making it accessible during runtime. Indirect usage of environment variables for SPI options and Quarkus properties is also vulnerable due to unconditional expansion by PropertyMapper logic, capturing sensitive data as default values in all Keycloak versions up to 26.0.2.	2024-11-25	5.9
CVE-2024-49596	dell - multiple products	Dell Wyse Management Suite, version WMS 4.4 and prior, contain a Missing Authorization vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Denial of service and arbitrary file deletion	2024-11-26	5.9
CVE-2024-11703	mozilla - Firefox	On Android, Firefox may have inadvertently allowed viewing saved passwords without the required device PIN authentication. This vulnerability affects Firefox < 133.	2024-11-26	5.7
CVE-2024-49351	ibm - Workload Scheduler	IBM Workload Scheduler 9.5, 10.1, and 10.2 stores user credentials in plain text which can be read by a local user.	2024-11-26	5.5
CVE-2024-52337	red hat - multiple products	A log spoofing flaw was found in the Tuned package due to improper sanitization of some API arguments. This flaw allows an attacker to pass a controlled sequence of characters; newlines can be inserted into the log. Instead of the 'evil' the attacker could mimic a valid TuneD log line and trick the administrator. The quotes '' are usually used in TuneD logs citing raw user input, so there will always be the ' character ending the spoofed input, and the administrator can easily overlook this. This logged string is later used in logging and in the output of utilities, for example, `tuned-adm get_instances` or other third-party programs that use Tuned's D-Bus interface for such operations.	2024-11-26	5.5
CVE-2024-9369	google - Chrome	Insufficient data validation in Mojo in Google Chrome prior to 129.0.6668.89 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	2024-11-27	5.5
CVE-2024-11695	mozilla - multiple products	A crafted URL containing Arabic script and whitespace characters could have hidden the true origin of the page, resulting in a potential spoofing attack. This vulnerability affects Firefox < 133, Firefox ESR < 128.5, Thunderbird < 133, and Thunderbird < 128.5.	2024-11-26	5.4
CVE-2024-11696	mozilla - multiple products	The application failed to account for exceptions thrown by the `loadManifestFromFile` method during add-on signature verification. This flaw, triggered by an invalid or unsupported extension manifest, could have caused runtime errors that disrupted the signature validation process. As a result, the enforcement of signature validation for unrelated add-ons may have been bypassed. Signature validation in this context is used to ensure that third-party applications on the user's computer have not tampered with the user's extensions, limiting the impact of this issue. This vulnerability affects Firefox < 133, Firefox ESR < 128.5, Thunderbird < 133, and Thunderbird < 128.5.	2024-11-26	5.4
CVE-2024-53975	mozilla - Firefox for iOS	Accessing a non-secure HTTP site that uses a non-existent port may cause the SSL padlock icon in the location URL bar to, misleadingly, appear secure. This vulnerability affects Firefox for iOS < 133.	2024-11-26	5.4
CVE-2024-53976	mozilla - Firefox for iOS	Under certain circumstances, navigating to a webpage would result in the address missing from the location URL bar, making it unclear what the URL was for the loaded webpage. This vulnerability affects Firefox for iOS < 133.	2024-11-26	5.4
CVE-2024-6538	red hat - Red Hat OpenShift Container Platform 4	A flaw was found in OpenShift Console. A Server Side Request Forgery (SSRF) attack can happen if an attacker supplies all or part of a URL to the server to query. The server is considered to be in a privileged network position and can often reach exposed services that aren't readily available to clients due to network filtering. Leveraging such an attack vector, the attacker can have an impact on other services and potentially disclose information or have other nefarious effects on the system. The /api/dev-console/proxy/internet endpoint on the OpenShit Console allows authenticated users to have the console's pod perform arbitrary and fully controlled HTTP(s) requests. The full response to these requests is returned by the endpoint. While the name of this endpoint suggests the requests are only bound to the internet, no such checks are in place. An authenticated user can therefore ask the console to perform arbitrary HTTP requests from outside the cluster to a service inside the cluster.	2024-11-25	5.3
CVE-2023-26280	ibm - Jazz Foundation	IBM Jazz Foundation 7.0.2 and 7.0.3 could allow a user to change their dashboard using a specially crafted HTTP request due to improper access control.	2024-11-25	5.3
CVE-2024-47249	apache software foundation - Apache NimBLE	Improper Validation of Array Index vulnerability in Apache NimBLE. Lack of input validation for HCI events from controller could result in out-of-bound memory corruption and crash. This issue requires broken or bogus Bluetooth controller and thus severity is considered low. This issue affects Apache NimBLE: through 1.7.0. Users are recommended to upgrade to version 1.8.0, which fixes the issue.	2024-11-26	5.0
CVE-2024-47250	apache software foundation - Apache NimBLE	Out-of-bounds Read vulnerability in Apache NimBLE. Missing proper validation of HCI advertising report could lead to out-of-bound access when parsing HCI event and thus bogus GAP 'device found' events being sent. This issue requires broken or bogus Bluetooth controller and thus severity is considered low. This issue affects Apache NimBLE: through 1.7.0. Users are recommended to upgrade to version 1.8.0, which fixes the issue.	2024-11-26	5.0
CVE-2024-11234	php - multiple products	In PHP versions 8.1.* before 8.1.31, 8.2.* before 8.2.26, 8.3.* before 8.3.14, when using streams with configured proxy and "request_fulluri" option, the URI is not properly sanitized which can lead to HTTP request smuggling and allow the attacker to use the proxy to perform arbitrary HTTP requests originating from the server, thus potentially gaining access to resources not normally available to the external user.	2024-11-24	4.8
CVE-2024-11233	php - multiple products	In PHP versions 8.1.* before 8.1.31, 8.2.* before 8.2.26, 8.3.* before 8.3.14, due to an error in convert.quoted-printable-decode filter certain data can lead to buffer overread by one byte, which can in certain circumstances lead to crashes or disclose content of other memory areas.	2024-11-24	4.8
CVE-2024-9666	red hat - multiple products	A vulnerability was found in the Keycloak Server. The Keycloak Server is vulnerable to a denial of service (DoS) attack due to improper handling of proxy headers. When Keycloak is configured to accept incoming proxy headers, it may accept non-IP values, such as obfuscated identifiers, without proper validation. This issue can lead to costly DNS resolution operations, which an attacker could exploit to tie up IO threads and potentially cause a denial of service. The attacker must have access to send requests to a Keycloak instance that is configured to accept	2024-11-25	4.7

		proxy headers, specifically when reverse proxies do not overwrite incoming headers, and Keycloak is configured to trust these headers.		
CVE-2024-42326	zabbix - Zabbix	There was discovered a use after free bug in browser.c in the es_browser_get_variant function	2024-11-27	4.4
CVE-2024-11692	mozilla - multiple products	An attacker could cause a select dropdown to be shown over another tab; this could have led to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 133, Firefox ESR < 128.5, Thunderbird < 133, and Thunderbird < 128.5.	2024-11-26	4.3
CVE-2024-11701	mozilla - multiple products	The incorrect domain may have been displayed in the address bar during an interrupted navigation attempt. This could have led to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 133 and Thunderbird < 133.	2024-11-26	4.3
CVE-2024-42332	zabbix - Zabbix	The researcher is showing that due to the way the SNMP trap log is parsed, an attacker can craft an SNMP trap with additional lines of information and have forged data show in the Zabbix UI. This attack requires SNMP auth to be off and/or the attacker to know the community/auth details. The attack requires an SNMP item to be configured as text on the target host.	2024-11-27	3.7
CVE-2024-42328	zabbix - Zabbix	When the webdriver for the Browser object downloads data from a HTTP server, the data pointer is set to NULL and is allocated only in curl_write_cb when receiving data. If the server's response is an empty document, then wd->data in the code below will remain NULL and an attempt to read from it will result in a crash.	2024-11-27	3.3
CVE-2024-42329	zabbix - Zabbix	The webdriver for the Browser object expects an error object to be initialized when the webdriver_session_query function fails. But this function can fail for various reasons without an error description and then the wd->error will be NULL and trying to read from it will result in a crash.	2024-11-27	3.3
CVE-2024-42331	zabbix - Zabbix	In the src/libs/zbxembed/browser.c file, the es_browser_ctor method retrieves a heap pointer from the Duktape JavaScript engine. This heap pointer is subsequently utilized by the browser_push_error method in the src/libs/zbxembed/browser_error.c file. A use-after-free bug can occur at this stage if the wd->browser heap pointer is freed by garbage collection.	2024-11-27	3.3
CVE-2024-36468	zabbix - Zabbix	The reported vulnerability is a stack buffer overflow in the zbx_snmp_cache_handle_engineid function within the Zabbix server/proxy code. This issue occurs when copying data from session->securityEngineID to local_record.engineid without proper bounds checking.	2024-11-27	3.0
CVE-2024-42333	zabbix - Zabbix	The researcher is showing that it is possible to leak a small amount of Zabbix Server memory using an out of bounds read in src/libs/zbxmedia/email.c	2024-11-27	2.7
CVE-2024-36464	zabbix - Zabbix	When exporting media types, the password is exported in the YAML in plain text. This appears to be a best practices type issue and may have no actual impact. The user would need to have permissions to access the media types and therefore would be expected to have access to these passwords.	2024-11-27	2.7
CVE-2024-22117	zabbix - Zabbix	When a URL is added to the map element, it is recorded in the database with sequential IDs. Upon adding a new URL, the system retrieves the last sysmapelementurlid value and increments it by one. However, an issue arises when a user manually changes the sysmapelementurlid value by adding sysmapelementurlid + 1. This action prevents others from adding URLs to the map element.	2024-11-26	2.2

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.