SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 19 July 2023

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-35189	Iagona ScrutisWeb versions 2.1.37 and prior are vulnerable to a remote code execution vulnerability that could allow an unauthenticated user to upload a malicious payload and execute it.	10.0	More Details
CVE-2023-3342	The User Registration plugin for WordPress is vulnerable to arbitrary file uploads due to a hardcoded encryption key and missing file type validation on the 'ur_upload_profile_pic' function in versions up to, and including, 3.0.2. This makes it possible for authenticated attackers with subscriber-level capabilities or above to upload arbitrary files on the affected site's server which may make remote code execution possible. This was partially patched in version 3.0.2 and fully patched in version 3.0.2.1.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37462	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Improper escaping in the document `SkinsCode.XWikiSkinsSheet` leads to an injection vector from view right on that document to programming rights, or in other words, it is possible to execute arbitrary script macros including Groovy and Python macros that allow remote code execution including unrestricted read and write access to all wiki contents. The attack works by opening a non-existing page with a name crafted to contain a dangerous payload. It is possible to check if an existing installation is vulnerable. See the linked GHSA for instructions on testing an installation. This issue has been patched in XWiki 14.4.8, 14.10.4 and 15.0-rc-1. Users are advised to upgrade. The fix commit `d9c88ddc` can also be applied manually to the impacted document `SkinsCode.XWikiSkinsSheet` and users unable to upgrade are advised to manually patch their installations.	9.9	More Details
CVE-2023-37718	Tenda F1202 V1.0BR_V1.2.0.20(408), FH1202_V1.2.0.19_EN were discovered to contain a stack overflow in the page parameter in the function fromSafeClientFilter.	9.8	More Details
CVE-2023-37721	Tenda F1202 V1.0BR_V1.2.0.20(408), FH1202_V1.2.0.19_EN were discovered to contain a stack overflow in the page parameter in the function fromSafeMacFilter.	9.8	More Details
CVE-2023-37793	WAYOS FBM-291W 19.09.11V was discovered to contain a buffer overflow via the component /upgrade_filter.asp.	9.8	More Details
CVE-2023-38336	netkit-rcp in rsh-client 0.17-24 allows command injection via filenames because /bin/sh is used by susystem, a related issue to CVE-2006-0225, CVE-2019-7283, and CVE-2020-15778.	9.8	More Details
CVE-2023-37723	Tenda F1202 V1.0BR_V1.2.0.20(408), FH1202_V1.2.0.19_EN were discovered to contain a stack overflow in the page parameter in the function fromqossetting.	9.8	More Details
CVE-2023-37722	Tenda F1202 V1.0BR_V1.2.0.20(408), FH1202_V1.2.0.19_EN were discovered to contain a stack overflow in the page parameter in the function fromSafeUrlFilter.	9.8	More Details
CVE-2023-37719	Tenda F1202 V1.0BR_V1.2.0.20(408), FH1202_V1.2.0.19_EN were discovered to contain a stack overflow in the page parameter in the function fromP2pListFilter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35802	IQ Engine before 10.6r1 on Extreme Network AP devices has a Buffer Overflow in the implementation of the CAPWAP protocol that may be exploited to obtain elevated privileges to conduct remote code execution. Access to the internal management interface/subnet is required to conduct the exploit.	9.8	More Details
CVE-2023-37582	The RocketMQ NameServer component still has a remote command execution vulnerability as the CVE-2023-33246 issue was not completely fixed in version 5.1.1. When NameServer address are leaked on the extranet and lack permission verification, an attacker can exploit this vulnerability by using the update configuration function on the NameServer component to execute commands as the system users that RocketMQ is running as. It is recommended for users to upgrade their NameServer version to 5.1.2 or above for RocketMQ 5.x or 4.9.7 or above for RocketMQ 4.x to prevent these attacks.	9.8	More Details
CVE-2023-37717	Tenda F1202 V1.0BR_V1.2.0.20(408) and FH1202_V1.2.0.19_EN, AC10 V1.0, AC1206 V1.0, AC7 V1.0, AC5 V1.0, and AC9 V3.0 were discovered to contain a stack overflow in the page parameter in the function fromDhcpListClient.	9.8	More Details
CVE-2023-37716	Tenda F1202 V1.0BR_V1.2.0.20(408) and FH1202_V1.2.0.19_EN, AC10 V1.0, AC1206 V1.0, AC7 V1.0, AC5 V1.0, and AC9 V3.0 were discovered to contain a stack overflow in the page parameter in the function fromNatStaticSetting.	9.8	More Details
CVE-2023-37715	Tenda F1202 V1.0BR_V1.2.0.20(408), FH1202_V1.2.0.19_EN were discovered to contain a stack overflow in the page parameter in the function frmL7ProtForm.	9.8	More Details
CVE-2023-37714	Tenda F1202 V1.0BR_V1.2.0.20(408), FH1202_V1.2.0.19_EN were discovered to contain a stack overflow in the page parameter in the function fromRouteStatic.	9.8	More Details
CVE-2023-37794	WAYOS FBM-291W 19.09.11V was discovered to contain a command injection vulnerability via the component /upgrade_filter.asp.	9.8	More Details
CVE-2023-30153	An SQL injection vulnerability in the Payplug (payplug) module for PrestaShop, in versions 3.6.0, 3.6.1, 3.6.2, 3.6.3, 3.7.0 and 3.7.1, allows remote attackers to execute arbitrary SQL commands via the ajax.php front controller.	9.8	More Details
CVE-2023-37839	An arbitrary file upload vulnerability in /dede/file_manage_control.php of DedeCMS v5.7.109 allows attackers to execute arbitrary code via uploading a crafted PHP file.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38378	The web interface on the RIGOL MSO5000 digital oscilloscope with firmware 00.01.03.00.03 allows remote attackers to execute arbitrary code via shell metacharacters in pass1 to the webcontrol changepwd.cgi application.	9.8	More Details
CVE-2023-3696	Prototype Pollution in GitHub repository automattic/mongoose prior to 7.3.4.	9.8	More Details
CVE-2023-26512	CWE-502 Deserialization of Untrusted Data at the rabbitmq-connector plugin module in Apache EventMesh (incubating) V1.7.0\V1.8.0 on windows\linux\mac os e.g. platforms allows attackers to send controlled message and remote code execute via rabbitmq messages. Users can use the code under the master branch in project repo to fix this issue, we will release the new version as soon as possible.	9.8	More Details
CVE-2023-2963	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Oliva Expertise Oliva Expertise EKS allows SQL Injection.This issue affects Oliva Expertise EKS: before 1.2.	9.8	More Details
CVE-2023-3186	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.	9.8	More Details
CVE-2023-3376	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Digital Strategy Zekiweb allows SQL Injection.This issue affects Zekiweb: before 2.	9.8	More Details
CVE-2023-2958	Authorization Bypass Through User-Controlled Key vulnerability in Origin Software ATS Pro allows Authentication Abuse, Authentication Bypass.This issue affects ATS Pro: before 20230714.	9.8	More Details
CVE-2023-37791	D-Link DIR-619L v2.04(TW) was discovered to contain a stack overflow via the curTime parameter at /goform/formLogin.	9.8	More Details
CVE-2021-37384	RCE (Remote Code Execution) vulnerability was found in some Furukawa ONU models, this vulnerability allows remote unauthenticated users to send arbitrary commands to the device via web interface.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37265	CasaOS is an open-source Personal Cloud system. Due to a lack of IP address verification an unauthenticated attackers can execute arbitrary commands as `root` on CasaOS instances. The problem was addressed by improving the detection of client IP addresses in `391dd7f`. This patch is part of CasaOS 0.4.4. Users should upgrade to CasaOS 0.4.4. If they can't, they should temporarily restrict access to CasaOS to untrusted users, for instance by not exposing it publicly.	9.8	More Details
CVE-2023-37266	CasaOS is an open-source Personal Cloud system. Unauthenticated attackers can craft arbitrary JWTs and access features that usually require authentication and execute arbitrary commands as `root` on CasaOS instances. This problem was addressed by improving the validation of JWTs in commit `705bf1f`. This patch is part of CasaOS 0.4.4. Users should upgrade to CasaOS 0.4.4. If they can't, they should temporarily restrict access to CasaOS to untrusted users, for instance by not exposing it publicly.	9.8	More Details
CVE-2023-36669	Missing Authentication for a Critical Function within the Kratos NGC Indoor Unit (IDU) before 11.4 allows remote attackers to obtain arbitrary control of the IDU/ODU system. Any attacker with layer-3 network access to the IDU can impersonate the Touch Panel Unit (TPU) within the IDU by sending crafted TCP requests to the IDU.	9.8	More Details
CVE-2023-38427	An issue was discovered in the Linux kernel before 6.3.8. fs/smb/server/smb2pdu.c in ksmbd has an integer underflow and out-of-bounds read in deassemble_neg_contexts.	9.8	More Details
CVE-2021-37522	SQL injection vulnerability in HKing2802 Locke-Bot 2.0.2 allows remote attackers to run arbitrary SQL commands via crafted string to /src/db.js, /commands/mute.js, /modules/event/messageDelete.js.	9.8	More Details
CVE-2023-37466	vm2 is an advanced vm/sandbox for Node.js. The library contains critical security issues and should not be used for production. The maintenance of the project has been discontinued. In vm2 for versions up to 3.9.19, `Promise` handler sanitization can be bypassed with the `@@species` accessor property allowing attackers to escape the sandbox and run arbitrary code, potentially allowing remote code execution inside the context of vm2 sandbox.	9.8	More Details
CVE-2023-30151	A SQL injection vulnerability in the Boxtal (envoimoinscher) module for PrestaShop, after version 3.1.10, allows remote attackers to execute arbitrary SQL commands via the `key` GET parameter.	9.8	More Details
CVE-2021-34123	An issue was discovered on atasm, version 1.09. A stack-buffer-overflow vulnerability in function aprintf() in asm.c allows attackers to execute arbitrary code on the system via a crafted file.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31704	Sourcecodester Online Computer and Laptop Store 1.0 is vulnerable to Incorrect Access Control, which allows remote attackers to elevate privileges to the administrator's role.	9.8	More Details
CVE-2023-33668	DigiExam up to v14.0.2 lacks integrity checks for native modules, allowing attackers to access PII and takeover accounts on shared computers.	9.8	More Details
CVE-2023-3595	Where this vulnerability exists in the Rockwell Automation 1756 EN2* and 1756 EN3* ControlLogix communication products, it could allow a malicious user to perform remote code execution with persistence on the target system through maliciously crafted CIP messages. This includes the ability to modify, deny, and exfiltrate data passing through the device.	9.8	More Details
CVE-2023-37627	Code-projects Online Restaurant Management System 1.0 is vulnerable to SQL Injection. Through SQL injection, an attacker can bypass the admin panel and view order records, add items, delete items etc.	9.8	More Details
CVE-2023-29300	Adobe ColdFusion versions 2018u16 (and earlier), 2021u6 (and earlier) and 2023.0.0.330468 (and earlier) are affected by a Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution. Exploitation of this issue does not require user interaction.	9.8	More Details
CVE-2023-37628	Online Piggery Management System 1.0 is vulnerable to SQL Injection.	9.8	More Details
CVE-2023-37629	Online Piggery Management System 1.0 is vulnerable to File Upload. An unauthenticated user can upload a php file by sending a POST request to "add-pig.php."	9.8	More Details
CVE-2023-26563	The Syncfusion EJ2 Node File Provider 0102271 is vulnerable to filesystem-server.js directory traversal. As a result, an unauthenticated attacker can: - On Windows, list files in any directory, read any file, delete any file, upload any file to any directory accessible by the web server. - On Linux, read any file, download any directory, delete any file, upload any file to any directory accessible by the web server.	9.8	More Details
CVE-2023-26564	The Syncfusion EJ2 ASPCore File Provider 3ac357f is vulnerable to Models/PhysicalFileProvider.cs directory traversal. As a result, an unauthenticated attacker can list files within a directory, download any file, or upload any file to any directory accessible by the web server.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33274	The authentication mechanism in PowerShield SNMP Web Pro 1.1 contains a vulnerability that allows unauthenticated users to directly access Common Gateway Interface (CGI) scripts without proper identification or authorization. This vulnerability arises from a lack of proper cookie verification and affects all instances of SNMP Web Pro 1.1 without HTTP Digest authentication enabled, regardless of the password used for the web interface.	9.8	More Details
CVE-2023-20918	In getPendingIntentLaunchFlags of ActivityOptions.java, there is a possible elevation of privilege due to a confused deputy with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2023-21250	In gatt_end_operation of gatt_utils.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2023-34124	The authentication mechanism in SonicWall GMS and Analytics Web Services had insufficient checks, allowing authentication bypass. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	9.8	More Details
CVE-2023-34128	Tomcat application credentials are hardcoded in SonicWall GMS and Analytics configuration file. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	9.8	More Details
CVE-2023-34130	SonicWall GMS and Analytics use outdated Tiny Encryption Algorithm (TEA) with a hardcoded key to encrypt sensitive data. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	9.8	More Details
CVE-2023-37567	Command injection vulnerability in ELECOM and LOGITEC wireless LAN routers allows a remote unauthenticated attacker to execute an arbitrary command by sending a specially crafted request to a certain port of the web management page. Affected products and versions are as follows: WRC-1167GHBK3-A v1.24 and earlier, WRC-F1167ACF2 all versions, WRC-600GHBK-A all versions, WRC-733FEBK2-A all versions, WRC-1467GHBK-A all versions, WRC-1900GHBK-A all versions, and LAN-W301NR all versions.	9.8	More Details
CVE-2023-34132	Use of password hash instead of password for authentication vulnerability in SonicWall GMS and Analytics allows Pass-the-Hash attacks. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34136	Vulnerability in SonicWall GMS and Analytics allows unauthenticated attacker to upload files to a restricted location not controlled by the attacker. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	9.8	More Details
CVE-2023-34137	SonicWall GMS and Analytics CAS Web Services application use static values for authentication without proper checks leading to authentication bypass vulnerability. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	9.8	More Details
CVE-2023-38198	acme.sh before 3.0.6 runs arbitrary commands from a remote server via eval, as exploited in the wild in June 2023.	9.8	More Details
CVE-2023-38199	coreruleset (aka OWASP ModSecurity Core Rule Set) through 3.3.4 does not detect multiple Content-Type request headers on some platforms. This might allow attackers to bypass a WAF with a crafted payload, aka "Content-Type confusion" between the WAF and the backend application. This occurs when the web application relies on only the last Content-Type header. Other platforms may reject the additional Content-Type header or merge conflicting headers, leading to detection as a malformed header.	9.8	More Details
CVE-2023-1547	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Elra Parkmatik allows SQL Injection through SOAP Parameter Tampering, Command Line Execution through SQL Injection.This issue affects Parkmatik: before 02.01-a51.	9.8	More Details
CVE-2023-2957	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Lisa Software Florist Site allows SQL Injection.This issue affects Florist Site: before 3.0.	9.8	More Details
CVE-2023-23585	Experion server DoS due to heap overflow occurring during the handling of a specially crafted message for a specific configuration operation. See Honeywell Security Notification for recommendations on upgrading and versioning.	9.8	More Details
CVE-2023-24480	Controller DoS due to stack overflow when decoding a message from the server. See Honeywell Security Notification for recommendations on upgrading and versioning.	9.8	More Details
CVE-2023-25078	Server or Console Station DoS due to heap overflow occurring during the handling of a specially crafted message for a specific configuration operation. See Honeywell Security Notification for recommendations on upgrading and versioning.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25178	Controller may be loaded with malicious firmware which could enable remote code execution. See Honeywell Security Notification for recommendations on upgrading and versioning.	9.8	More Details
CVE-2023-25770	Controller DoS may occur due to buffer overflow when an error is generated in response to a specially crafted message. See Honeywell Security Notification for recommendations on upgrading and versioning.	9.8	More Details
CVE-2023-36670	A remotely exploitable command injection vulnerability was found on the Kratos NGC-IDU 9.1.0.4. An attacker can execute arbitrary Linux commands as root by sending crafted TCP requests to the device.	9.8	More Details
CVE-2023-35070	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in VegaGroup Web Collection allows SQL Injection.This issue affects Web Collection: before 31197.	9.8	More Details
CVE-2023-38429	An issue was discovered in the Linux kernel before 6.3.4. fs/ksmbd/connection.c in ksmbd has an off-by-one error in memory allocation (because of ksmbd_smb2_check_message) that may lead to out-of-bounds access.	9.8	More Details
CVE-2023-30429	Incorrect Authorization vulnerability in Apache Software Foundation Apache Pulsar. This issue affects Apache Pulsar: before 2.10.4, and 2.11.0. When a client connects to the Pulsar Function Worker via the Pulsar Proxy where the Pulsar Proxy uses mTLS authentication to authenticate with the Pulsar Function Worker, the Pulsar Function Worker incorrectly performs authorization by using the Proxy's role for authorization instead of the client's role, which can lead to privilege escalation, especially if the proxy is configured with a superuser role. The recommended mitigation for impacted users is to upgrade the Pulsar Function Worker to a patched version. 2.10 Pulsar Function Worker users should upgrade to at least 2.10.4. 2.11 Pulsar Function Worker users should upgrade to at least 2.11.1. 3.0 Pulsar Function Worker users are unaffected. Any users running the Pulsar Function Worker for 2.9.* and earlier should upgrade to one of the above patched versions.	9.6	More Details
CVE-2023-2507	CleverTap Cordova Plugin version 2.6.2 allows a remote attacker to execute JavaScript code in any application that is opened via a specially constructed deeplink by an attacker. This is possible because the plugin does not correctly validate the data coming from the deeplinks before using them.	9.3	More Details
CVE-2023-38431	An issue was discovered in the Linux kernel before 6.3.8. fs/smb/server/connection.c in ksmbd does not validate the relationship between the NetBIOS header's length field and the SMB header sizes, via pdu_size in ksmbd_conn_handler_loop, leading to an out-of-bounds read.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38432	An issue was discovered in the Linux kernel before 6.3.10. fs/smb/server/smb2misc.c in ksmbd does not validate the relationship between the command payload size and the RFC1002 length specification, leading to an out-of-bounds read.	9.1	More Details
CVE-2023-38430	An issue was discovered in the Linux kernel before 6.3.9. ksmbd does not validate the SMB request protocol ID, leading to an out-of-bounds read.	9.1	More Details
CVE-2023-38428	An issue was discovered in the Linux kernel before 6.3.4. fs/ksmbd/smb2pdu.c in ksmbd does not properly check the UserName value because it does not consider the address of security buffer, leading to an out-of-bounds read.	9.1	More Details
CVE-2023-34329	AMI MegaRAC SPx12 contains a vulnerability in BMC where a User may cause an authentication bypass by spoofing the HTTP header. A successful exploit of this vulnerability may lead to loss of confidentiality, integrity, and availability.	9.1	More Details
CVE-2023-38426	An issue was discovered in the Linux kernel before 6.3.4. ksmbd has an out-of-bounds read in smb2_find_context_vals when create_context's name_len is larger than the tag length.	9.1	More Details
CVE-2023-3724	If a TLS 1.3 client gets neither a PSK (pre shared key) extension nor a KSE (key share extension) when connecting to a malicious server, a default predictable buffer gets used for the IKM (Input Keying Material) value when generating the session master secret. Using a potentially known IKM value when generating the session master secret key compromises the key generated, allowing an eavesdropper to reconstruct it and potentially allowing access to or meddling with message contents in the session. This issue does not affect client validation of connected servers, nor expose private key information, but could result in an insecure TLS 1.3 session when not controlling both sides of the connection. wolfSSL recommends that TLS 1.3 client side users update the version of wolfSSL used.	9.1	More Details
CVE-2023-2003	Embedded malicious code vulnerability in Vision1210, in the build 5 of operating system version 4.3, which could allow a remote attacker to store base64-encoded malicious code in the device's data tables via the PCOM protocol, which can then be retrieved by a client and executed on the device.	9.1	More Details
CVE-2023-34142	Cleartext Transmission of Sensitive Information vulnerability in Hitachi Device Manager on Windows, Linux (Device Manager Server, Device Manager Agent, Host Data Collector components) allows Interception.This issue affects Hitachi Device Manager: before 8.8.5-02.	9.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21974	Vulnerability in the Application Express Team Calendar Plugin product of Oracle Application Express (component: User Account). Supported versions that are affected are Application Express Team Calendar Plugin: 18.2-22.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Application Express Team Calendar Plugin. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Application Express Team Calendar Plugin, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Application Express Team Calendar Plugin. CVSS 3.1 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H).	9.0	More Details
CVE-2023-21975	Vulnerability in the Application Express Customers Plugin product of Oracle Application Express (component: User Account). Supported versions that are affected are Application Express Customers Plugin: 18.2-22.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Application Express Customers Plugin. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Application Express Customers Plugin, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Application Express Customers Plugin. CVSS 3.1 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H).	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference

CVE Number	Description	Base Score	Reference
CVE-2023-22508	This High severity RCE (Remote Code Execution) vulnerability known as CVE-2023-22508 was introduced in version 6.1.0 of Confluence Data Center & Server. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 8.5, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and no user interaction. Atlassian recommends that you upgrade your instance to avoid this bug using the following options: * Upgrade to a Confluence feature release greater than or equal to 8.2.0 (ie: 8.2, 8.2, 8.4, etc...) * Upgrade to a Confluence 7.19 LTS bugfix release greater than or equal to 7.19.8 (ie: 7.19.8, 7.19.9, 7.19.10, 7.19.11, etc...) * Upgrade to a Confluence 7.13 LTS bugfix release greater than or equal to 7.13.20 (Release available early August) See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Data Center & Server from the download center (https://www.atlassian.com/software/confluence/download-archives). If you are unable to upgrade your instance please use the following guide to workaround the issue https://confluence.atlassian.com/confkb/how-to-disable-the-jmx-network-port-for-cve-2023-22508-1267761550.html This vulnerability was discovered by a private user and reported via our Bug Bounty program.	8.8	More Details
CVE-2023-33011	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled.	8.8	More Details
CVE-2023-3105	The LearnDash LMS plugin for WordPress is vulnerable to Insecure Direct Object References in versions up to, and including, 4.6.0. This is due to the plugin providing user-controlled access to objects, letting a user bypass authorization and access system resources. This makes it possible for attackers with with existing account access at any level, to change user passwords and potentially take over administrator accounts.	8.8	More Details
CVE-2023-2759	A hidden API exists in TapHome's core platform before version 2023.2 that allows an authenticated, low privileged user to change passwords of other users without any prior knowledge. The attacker may gain full access to the device by using this vulnerability.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2329	The WooCommerce Google Sheet Connector WordPress plugin before 1.3.6 does not have CSRF check when updating its Access Code, which could allow attackers to make logged in admin change the access code to an arbitrary one via a CSRF attack	8.8	More Details
CVE-2023-2330	The Caldera Forms Google Sheets Connector WordPress plugin before 1.3 does not have CSRF check when updating its Access Code, which could allow attackers to make logged in admin change the access code to an arbitrary one via a CSRF attack	8.8	More Details
CVE-2023-2636	The AN_GradeBook WordPress plugin through 5.0.1 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as subscriber	8.8	More Details
CVE-2023-3179	The POST SMTP Mailer WordPress plugin before 2.5.7 does not have proper CSRF checks in some AJAX actions, which could allow attackers to make logged in users with the manage_postman_smtp capability resend an email to an arbitrary address (for example a password reset email could be resent to an attacker controlled email, and allow them to take over an account).	8.8	More Details
CVE-2023-28767	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled.	8.8	More Details
CVE-2023-33012	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37196	A CWE-89: Improper Neutralization of Special Elements vulnerability used in an SQL Command ('SQL Injection') vulnerability exists that could allow a user already authenticated on DCE to access unauthorized content, change, or delete content, or perform unauthorized actions when tampering with the alert settings of endpoints on DCE.	8.8	More Details
CVE-2023-34139	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device.	8.8	More Details
CVE-2023-3713	The ProfileGrid plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'profile_magic_check_smtp_connection' function in versions up to, and including, 5.5.1. This makes it possible for authenticated attackers, with subscriber-level permissions or above to update the site options arbitrarily. This can be used by attackers to achieve privilege escalation.	8.8	More Details
CVE-2022-26563	An issue was discovered in Tildeslash Monit before 5.31.0, allows remote attackers to gain escilated privlidges due to improper PAM-authorization.	8.8	More Details
CVE-2023-32200	There is insufficient restrictions of called script functions in Apache Jena versions 4.8.0 and earlier. It allows a remote user to execute javascript via a SPARQL query. This issue affects Apache Jena: from 3.7.0 through 4.8.0.	8.8	More Details
CVE-2020-22159	EVERTZ devices 3080IPX exe-guest-v1.2-r26125, 7801FC 1.3 Build 27, and 7890IXG V494 are vulnerable to Arbitrary File Upload, allowing an authenticated attacker to upload a webshell or overwrite any critical system files.	8.8	More Details
CVE-2022-34155	Improper Authentication vulnerability in miniOrange OAuth Single Sign On – SSO (OAuth Client) plugin allows Authentication Bypass.This issue affects OAuth Single Sign On – SSO (OAuth Client): from n/a through 6.23.3.	8.8	More Details
CVE-2023-33265	In Hazelcast through 5.0.4, 5.1 through 5.1.6, and 5.2 through 5.2.3, executor services don't check client permissions properly, allowing authenticated users to execute tasks on members without the required permissions granted.	8.8	More Details
CVE-2023-38349	PNP4Nagios through 81ebfc5 lacks CSRF protection in the AJAX controller. This affects 0.6.26.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37197	A CWE-89: Improper Neutralization of Special Elements vulnerability used in an SQL Command ('SQL Injection') vulnerability exists that could allow a user already authenticated on DCE to access unauthorized content, change, or delete content, or perform unauthorized actions when tampering with the mass configuration settings of endpoints on DCE.	8.8	More Details
CVE-2023-37964	A cross-site request forgery (CSRF) vulnerability in Jenkins ElasticBox CI Plugin 5.0.1 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	8.8	More Details
CVE-2023-34126	Vulnerability in SonicWall GMS and Analytics allows an authenticated attacker to upload files on the underlying filesystem with root privileges. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	8.8	More Details
CVE-2023-3600	During the worker lifecycle, a use-after-free condition could have occured, which could have led to a potentially exploitable crash. This vulnerability affects Firefox < 115.0.2, Firefox ESR < 115.0.2, and Thunderbird < 115.0.1.	8.8	More Details
CVE-2023-37415	Improper Input Validation vulnerability in Apache Software Foundation Apache Airflow Apache Hive Provider. Patching on top of CVE-2023-35797 Before 6.1.2 the proxy_user option can also inject semicolon. This issue affects Apache Airflow Apache Hive Provider: before 6.1.2. It is recommended updating provider version to 6.1.2 in order to avoid this vulnerability.	8.8	More Details
CVE-2023-37946	Jenkins OpenShift Login Plugin 1.1.0.227.v27e08dfb_1a_20 and earlier does not invalidate the previous session on login.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22505	This High severity RCE (Remote Code Execution) vulnerability known as CVE-2023-22505 was introduced in version 8.0.0 of Confluence Data Center & Server. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 8, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and no user interaction. Atlassian recommends that you upgrade your instance to latest version. If you're unable to upgrade to latest, upgrade to one of these fixed versions: 8.3.2, 8.4.0. See the release notes ([https://confluence.atlassian.com/doc/confluence-release-notes-327.html).lhttps://confluence.atlassian.com/doc/confluence-release-notes-327.html).] You can download the latest version of Confluence Data Center & Server from the download center ([https://www.atlassian.com/software/confluence/download-archives).lhttps://www.atlassian.com/software/confluence/download-archives).] This vulnerability was discovered by a private user and reported via our Bug Bounty program.	8.8	More Details
CVE-2023-3343	The User Registration plugin for WordPress is vulnerable to PHP Object Injection in versions up to, and including, 3.0.1 via deserialization of untrusted input from the 'profile-pic-url' parameter. This allows authenticated attackers, with subscriber-level permissions and above, to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	8.8	More Details
CVE-2023-37957	A cross-site request forgery (CSRF) vulnerability in Jenkins Pipeline restFul API Plugin 0.11 and earlier allows attackers to connect to an attacker-specified URL, capturing a newly generated JCLI token.	8.8	More Details
CVE-2023-37958	A cross-site request forgery (CSRF) vulnerability in Jenkins Sumologic Publisher Plugin 2.2.1 and earlier allows attackers to connect to an attacker-specified URL.	8.8	More Details
CVE-2023-37961	A cross-site request forgery (CSRF) vulnerability in Jenkins Assembla Auth Plugin 1.14 and earlier allows attackers to trick users into logging in to the attacker's account.	8.8	More Details
CVE-2023-37962	A cross-site request forgery (CSRF) vulnerability in Jenkins Benchmark Evaluator Plugin 1.0.1 and earlier allows attackers to connect to an attacker-specified URL and to check for the existence of directories, `.csv`, and `.ycsb` files on the Jenkins controller file system.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37562	Cross-site request forgery (CSRF) vulnerability in exists in WTC-C1167GC-B v1.17 and earlier, and WTC-C1167GC-W v1.17 and earlier. If a user views a malicious page while logged in, unintended operations may be performed.	8.8	More Details
CVE-2023-34129	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in SonicWall GMS and Analytics allows an authenticated remote attacker to traverse the directory and extract arbitrary files using Zip Slip method to any location on the underlying filesystem with root privileges. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	8.8	More Details
CVE-2023-34127	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in SonicWall GMS, SonicWall Analytics enables an authenticated attacker to execute arbitrary code with root privileges. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	8.8	More Details
CVE-2023-37464	OpenIDC/cjose is a C library implementing the Javascript Object Signing and Encryption (JOSE). The AES GCM decryption routine incorrectly uses the Tag length from the actual Authentication Tag provided in the JWE. The spec says that a fixed length of 16 octets must be applied. Therefore this bug allows an attacker to provide a truncated Authentication Tag and to modify the JWE accordingly. Users should upgrade to a version >= 0.6.2.2. Users unable to upgrade should avoid using AES GCM encryption and replace it with another encryption algorithm (e.g. AES CBC).	8.6	More Details
CVE-2023-37473	zenstruck/collections is a set of helpers for iterating/paginating/filtering collections. Passing _callable strings_ (ie `system`) caused the function to be executed. This would result in a limited subset of specific user input being executed as if it were code. This issue has been addressed in commit `f4b1c48820` and included in release version 0.2.1. Users are advised to upgrade. Users unable to upgrade should ensure that user input is not passed to either `EntityRepository::find()` or `query()`.	8.5	More Details
CVE-2023-23660	Auth. (subscriber+) SQL Injection (SQLi) vulnerability in MainWP MainWP Maintenance Extension plugin <= 4.1.1 versions.	8.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22062	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Repository). The supported version that is affected is 11.2.13.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. While the vulnerability is in Oracle Hyperion Financial Reporting, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Reporting accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Financial Reporting. CVSS 3.1 Base Score 8.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:L).	8.5	More Details
CVE-2023-29450	JavaScript pre-processing can be used by the attacker to gain access to the file system (read-only access on behalf of user "zabbix") on the Zabbix Server or Zabbix Proxy, potentially leading to unauthorized access to sensitive data.	8.5	More Details
CVE-2023-34236	Weave GitOps Terraform Controller (aka Weave TF-controller) is a controller for Flux to reconcile Terraform resources in a GitOps way. A vulnerability has been identified in Weave GitOps Terraform Controller which could allow an authenticated remote attacker to view sensitive information. This vulnerability stems from Weave GitOps Terraform Runners (`tf-runner`), where sensitive data is inadvertently printed - potentially revealing sensitive user data in their pod logs. In particular, functions `tfexec.ShowPlan`, `tfexec.ShowPlanRaw`, and `tfexec.Output` are implicated when the `tfexec` object set its `Stdout` and `Stderr` to be `os.Stdout` and `os.Stderr`. An unauthorized remote attacker could exploit this vulnerability by accessing these prints of sensitive information, which may contain configurations or tokens that could be used to gain unauthorized control or access to resources managed by the Terraform controller. A successful exploit could allow the attacker to utilize this sensitive data, potentially leading to unauthorized access or control of the system. This vulnerability has been addressed in Weave GitOps Terraform Controller versions `v0.14.4` and `v0.15.0-rc.5`. Users are urged to upgrade to one of these versions to mitigate the vulnerability. As a temporary measure until the patch can be applied, users can add the environment variable `DISABLE_TF_LOGS` to the tf-runners via the runner pod template of the Terraform Custom Resource. This will prevent the logging of sensitive information and mitigate the risk of this vulnerability.	8.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22014	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.59 and 8.60. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where PeopleSoft Enterprise PeopleTools executes to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 8.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	8.4	More Details
CVE-2023-30989	IBM Performance Tools for i 7.2, 7.3, 7.4, and 7.5 contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain all object access to the host operating system. IBM X-Force ID: 254017.	8.4	More Details
CVE-2023-30988	The IBM i 7.2, 7.3, 7.4, and 7.5 product Facsimile Support for i contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain root access to the host operating system. IBM X-Force ID: 254016.	8.4	More Details
CVE-2023-30563	A malicious file could be uploaded into a System Manager User Import Function resulting in a hijacked session.	8.2	More Details
CVE-2023-37579	Incorrect Authorization vulnerability in Apache Software Foundation Apache Pulsar Function Worker. This issue affects Apache Pulsar: before 2.10.4, and 2.11.0. Any authenticated user can retrieve a source's configuration or a sink's configuration without authorization. Many sources and sinks contain credentials in the configuration, which could lead to leaked credentials. This vulnerability is mitigated by the fact that there is not a known way for an authenticated user to enumerate another tenant's sources or sinks, meaning the source or sink name would need to be guessed in order to exploit this vulnerability. The recommended mitigation for impacted users is to upgrade the Pulsar Function Worker to a patched version. 2.10 Pulsar Function Worker users should upgrade to at least 2.10.4. 2.11 Pulsar Function Worker users should upgrade to at least 2.11.1. 3.0 Pulsar Function Worker users are unaffected. Any users running the Pulsar Function Worker for 2.9.* and earlier should upgrade to one of the above patched versions.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30428	Incorrect Authorization vulnerability in Apache Software Foundation Apache Pulsar Broker's Rest Producer allows authenticated user with a custom HTTP header to produce a message to any topic using the broker's admin role. This issue affects Apache Pulsar Brokers: from 2.9.0 through 2.9.5, from 2.10.0 before 2.10.4, 2.11.0. The vulnerability is exploitable when an attacker can connect directly to the Pulsar Broker. If an attacker is connecting through the Pulsar Proxy, there is no known way to exploit this authorization vulnerability. There are two known risks for affected users. First, an attacker could produce garbage messages to any topic in the cluster. Second, an attacker could produce messages to the topic level policies topic for other tenants and influence topic settings that could lead to exfiltration and/or deletion of messages for other tenants. 2.8 Pulsar Broker users and earlier are unaffected. 2.9 Pulsar Broker users should upgrade to one of the patched versions. 2.10 Pulsar Broker users should upgrade to at least 2.10.4. 2.11 Pulsar Broker users should upgrade to at least 2.11.1. 3.0 Pulsar Broker users are unaffected.	8.2	More Details
CVE-2023-34330	AMI SPx contains a vulnerability in the BMC where a user may inject code which could be executed via a Dynamic Redfish Extension interface. A successful exploit of this vulnerability may lead to a loss of confidentiality, integrity, and availability.	8.2	More Details
CVE-2023-32761	Cross Site Request Forgery (CSRF) vulnerability in Archer Platform before v.6.13 and fixed in v.6.12.0.6 and v.6.13.0 allows an authenticated attacker to execute arbitrary code via a crafted request.	8.1	More Details
CVE-2023-22018	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.46 and Prior to 7.0.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via RDP to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37273	Auto-GPT is an experimental open-source application showcasing the capabilities of the GPT-4 language model. Running Auto-GPT version prior to 0.4.3 by cloning the git repo and executing `docker compose run auto-gpt` in the repo root uses a different docker-compose.yml file from the one suggested in the official docker set up instructions. The docker-compose.yml file located in the repo root mounts itself into the docker container without write protection. This means that if malicious custom python code is executed via the `execute_python_file` and `execute_python_code` commands, it can overwrite the docker-compose.yml file and abuse it to gain control of the host system the next time Auto-GPT is started. The issue has been patched in version 0.4.3.	8.1	More Details
CVE-2023-3633	An out-of-bounds write vulnerability in Bitdefender Engines on Windows causes the engine to crash. This issue affects Bitdefender Engines version 7.94791 and lower.	8.1	More Details
CVE-2023-3615	Mattermost iOS app fails to properly validate the server certificate while initializing the TLS connection allowing a network attacker to intercept the WebSockets connection.	8.1	More Details
CVE-2023-37568	ELECOM wireless LAN routers WRC-1167GHBK-S v1.03 and earlier, and WRC-1167GEBK-S v1.03 and earlier allow a network-adjacent authenticated attacker to execute an arbitrary command by sending a specially crafted request to the web management page.	8.0	More Details
CVE-2023-37566	Command injection vulnerability in ELECOM and LOGITEC wireless LAN routers allows a network-adjacent authenticated attacker to execute an arbitrary command by sending a specially crafted request to the web management page. Affected products and versions are as follows: WRC-1167GHBK3-A v1.24 and earlier, WRC-1167FEBK-A v1.18 and earlier, WRC-F1167ACF2 all versions, WRC-600GHBK-A all versions, WRC-733FEBK2-A all versions, WRC-1467GHBK-A all versions, WRC-1900GHBK-A all versions, and LAN-W301NR all versions.	8.0	More Details
CVE-2023-37565	Code injection vulnerability in ELECOM wireless LAN routers allows a network-adjacent authenticated attacker to execute arbitrary code by sending a specially crafted request. Affected products and versions are as follows: WRC-1167GHBK-S v1.03 and earlier, WRC-1167GEBK-S v1.03 and earlier, WRC-1167FEBK-S v1.04 and earlier, WRC-1167GHBK3-A v1.24 and earlier, and WRC-1167FEBK-A v1.18 and earlier.	8.0	More Details
CVE-2022-45855	SpringEL injection in the metrics source in Apache Ambari version 2.7.0 to 2.7.6 allows a malicious authenticated user to execute arbitrary code remotely. Users are recommended to upgrade to 2.7.7.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42009	SpringEL injection in the server agent in Apache Ambari version 2.7.0 to 2.7.6 allows a malicious authenticated user to execute arbitrary code remotely. Users are recommended to upgrade to 2.7.7.	8.0	More Details
CVE-2023-34138	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance.	8.0	More Details
CVE-2023-34141	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance.	8.0	More Details
CVE-2023-37564	OS command injection vulnerability in ELECOM wireless LAN routers allows a network-adjacent authenticated attacker to execute an arbitrary OS command with a root privilege by sending a specially crafted request. Affected products and versions are as follows: WRC-1167GHBK-S v1.03 and earlier, WRC-1167GEBK-S v1.03 and earlier, WRC-1167FEBK-S v1.04 and earlier, WRC-1167GHBK3-A v1.24 and earlier, and WRC-1167FEBK-A v1.18 and earlier.	8.0	More Details
CVE-2023-29308	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22023	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Device Driver Interface). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in takeover of Oracle Solaris. Note: CVE-2023-22023 is equivalent to CVE-2023-31284. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	7.8	More Details
CVE-2022-33065	Multiple signed integers overflow in function au_read_header in src/au.c and in functions mat4_open and mat4_read_header in src/mat4.c in Libsndfile, allows an attacker to cause Denial of Service or other unspecified impacts.	7.8	More Details
CVE-2023-21257	In updateSettingsInternalLI of InstallPackageHelper.java, there is a possible way to sideload an app in the work profile 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.	7.8	More Details
CVE-2023-21256	In SettingsHomepageActivity.java, there is a possible way to launch arbitrary activities via Settings due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.8	More Details
CVE-2023-21255	In multiple functions of binder.c, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-21254	In getCurrentState of OneTimePermissionUserManager.java, there is a possible way to hold one-time permissions after the app is being killed due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-21248	In getAvailabilityStatus of WifiScanningMainSwitchPreferenceController.java, there is a possible way to bypass a device policy restriction 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.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21247	In getAvailabilityStatus of BluetoothScanningMainSwitchPreferenceController.java, there is a possible way to bypass a device policy restriction 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.	7.8	More Details
CVE-2023-21241	In rw_i93_send_to_upper of rw_i93.cc, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-21145	In updatePictureInPictureMode of ActivityRecord.java, there is a possible bypass of background launch restrictions due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-3513	Improper Privilege Control in RazerCentralSerivce Named Pipe in Razer RazerCentral <=7.11.0.558 on Windows allows a malicious actor with local access to gain SYSTEM privilege via communicating with the named pipe as a low-privilege user and triggering an insecure .NET deserialization.	7.8	More Details
CVE-2023-3514	Improper Privilege Control in RazerCentralSerivce Named Pipe in Razer RazerCentral <=7.11.0.558 on Windows allows a malicious actor with local access to gain SYSTEM privilege via communicating with the named pipe as a low-privilege user and calling "AddModule" or "UninstallModules" command to execute arbitrary executable file.	7.8	More Details
CVE-2023-35692	In getLocationCache of GeoLocation.java, there is a possible way to send a mock location during an emergency call due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-29414	A CWE-120: Buffer Copy without Checking Size of Input (Classic Buffer Overflow) vulnerability exists that could cause user privilege escalation if a local user sends specific string input to a local function call.	7.8	More Details
CVE-2023-2763	Use-After-Free, Out-of-bounds Write and Heap-based Buffer Overflow vulnerabilities exist in the DWG and DXF file reading procedure in SOLIDWORKS Desktop from Release SOLIDWORKS 2021 through Release SOLIDWORKS 2023. These vulnerabilities could allow an attacker to execute arbitrary code while opening a specially crafted DWG or DXF file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2762	A Use-After-Free vulnerability in SLDPRT file reading procedure exists in SOLIDWORKS Desktop from Release SOLIDWORKS 2021 through Release SOLIDWORKS 2023. This vulnerability could allow an attacker to execute arbitrary code while opening a specially crafted SLDPRT file.	7.8	More Details
CVE-2023-36887	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-43757	Adobe Media Encoder versions 22.0, 15.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious 3GP file	7.8	More Details
CVE-2023-21399	there is a possible way to bypass cryptographic assurances due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-21245	In showNextSecurityScreenOrFinish of KeyguardSecurityContainerController.java, there is a possible way to access the lock screen during device setup due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-30917	In DMService, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	7.8	More Details
CVE-2022-33064	An off-by-one error in function wav_read_header in src/wav.c in Libsndfile 1.1.0, results in a write out of bound, which allows an attacker to execute arbitrary code, Denial of Service or other unspecified impacts.	7.8	More Details
CVE-2023-30928	In telephony service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	7.8	More Details
CVE-2023-30929	In telephony service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	7.8	More Details
CVE-2023-30916	In DMService, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34119	A flaw was discovered in htmodoc 1.9.12 in function parse_paragraph in ps-pdf.cxx ,this flaw possibly allows possible code execution and a denial of service via a crafted file.	7.8	More Details
CVE-2021-34121	An Out of Bounds flaw was discovered in htmodoc 1.9.12 in function parse_tree() in toc.cxx, this possibly leads to memory layout information leaking in the data. This might be used in a chain of vulnerability in order to reach code execution.	7.8	More Details
CVE-2023-32760	An issue in Archer Platform before v.6.13 fixed in v.6.12.0.6 and v.6.13.0 allows an authenticated attacker to obtain sensitive information via API calls related to data feeds and data publication.	7.7	More Details
CVE-2023-37472	Knowage is an open source suite for business analytics. The application often use user supplied data to create HQL queries without prior sanitization. An attacker can create specially crafted HQL queries that will break subsequent SQL queries generated by the Hibernate engine. The endpoint `_/knowage/restful-services/2.0/documents/listDocument_` calls the `_countBIObjects_` method of the `_BIObjectDAOHibImpl_` object with the user supplied `_label_` parameter without prior sanitization. This can lead to SQL injection in the backing database. Other injections have been identified in the application as well. An authenticated attacker with low privileges could leverage this vulnerability in order to retrieve sensitive information from the database, such as account credentials or business information. This issue has been addressed in version 8.1.8. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.7	More Details
CVE-2023-2760	An SQL injection vulnerability exists in TapHome core HandleMessageUpdateDevicePropertiesRequest function before version 2023.2, allowing low privileged users to inject arbitrary SQL directives into an SQL query and execute arbitrary SQL commands and get full reading access. This may also lead to limited write access and temporary Denial-of-Service.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22060	Vulnerability in the Oracle Hyperion Workspace product of Oracle Hyperion (component: UI and Visualization). The supported version that is affected is 11.2.13.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Workspace. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Workspace accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Workspace accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Workspace. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:L).	7.6	More Details
CVE-2023-36831	An Improper Check or Handling of Exceptional Conditions vulnerability in the UTM (Unified Threat Management) Web-Filtering feature of Juniper Networks Junos OS on SRX Series causes a jbuf memory leak to occur when accessing certain websites, eventually leading to a Denial of Service (DoS) condition. Service restoration is only possible by rebooting the system. The jbuf memory leak only occurs in SSL Proxy and UTM Web-Filtering configurations. Other products, platforms, and configurations are not affected by this vulnerability. This issue affects Juniper Networks Junos OS on SRX Series: 22.2 versions prior to 22.2R3; 22.3 versions prior to 22.3R2-S1, 22.3R3; 22.4 versions prior to 22.4R1-S2, 22.4R2. This issue does not affect Juniper Networks Junos OS versions prior to 22.2R2.	7.5	More Details
CVE-2023-35069	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Bullwark allows Path Traversal.This issue affects Bullwark: before BLW-2016E-960H.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36832	An Improper Handling of Exceptional Conditions vulnerability in packet processing of Juniper Networks Junos OS on MX Series allows an unauthenticated network-based attacker to send specific packets to an Aggregated Multiservices (AMS) interface on the device, causing the packet forwarding engine (PFE) to crash, resulting in a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue is only triggered by packets destined to a local-interface via a service-interface (AMS). AMS is only supported on the MS-MPC, MS-MIC, and MX-SPC3 cards. This issue is not experienced on other types of interfaces or configurations. Additionally, transit traffic does not trigger this issue. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S12; 20.2 versions prior to 20.2R3-S8; 20.4 versions prior to 20.4R3-S7; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S5; 21.3 versions prior to 21.3R3-S4; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S2; 22.2 versions prior to 22.2R3; 22.3 versions prior to 22.3R2-S1, 22.3R3; 22.4 versions prior to 22.4R1-S2, 22.4R2.	7.5	More Details
CVE-2023-28985	An Improper Validation of Syntactic Correctness of Input vulnerability in Intrusion Detection and Prevention (IDP) of Juniper Networks SRX Series and MX Series allows an unauthenticated, network-based attacker to cause Denial of Service (DoS). Continued receipt of this specific packet will cause a sustained Denial of Service condition. On all SRX Series and MX Series platforms, where IDP is enabled and a specific malformed SSL packet is received, the SSL detector crashes leading to an FPC core. This issue affects Juniper Networks SRX Series and MX Series prior to SigPack 3598. In order to identify the current SigPack version, following command can be used: user@junos# show security idp security-package-version	7.5	More Details
CVE-2023-32759	An issue in Archer Platform before v.6.13 and fixed in 6.12.0.6 and 6.13.0 allows an authenticated attacker to obtain sensitive information via a crafted URL.	7.5	More Details
CVE-2023-3424	An issue has been discovered in GitLab CE/EE affecting all versions starting from 10.3 before 15.11.10, all versions starting from 16.0 before 16.0.6, all versions starting from 16.1 before 16.1.1. A Regular Expression Denial of Service was possible via sending crafted payloads to the preview_markdown endpoint.	7.5	More Details
CVE-2023-31820	An issue found in Shizutetsu Store v.13.6.1 allows a remote attacker to gain access to sensitive information via the channel access token in the miniapp function.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29301	Adobe ColdFusion versions 2018u16 (and earlier), 2021u6 (and earlier) and 2023.0.0.330468 (and earlier) are affected by an Improper Restriction of Excessive Authentication Attempts vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to impact the confidentiality of the user. Exploitation of this issue does not require user interaction.	7.5	More Details
CVE-2023-37274	Auto-GPT is an experimental open-source application showcasing the capabilities of the GPT-4 language model. When Auto-GPT is executed directly on the host system via the provided run.sh or run.bat files, custom Python code execution is sandboxed using a temporary dedicated docker container which should not have access to any files outside of the Auto-GPT workspace directory. Before v0.4.3, the `execute_python_code` command (introduced in v0.4.1) does not sanitize the `basename` arg before writing LLM-supplied code to a file with an LLM-supplied name. This allows for a path traversal attack that can overwrite any .py file outside the workspace directory by specifying a `basename` such as `../../../main.py`. This can further be abused to achieve arbitrary code execution on the host running Auto-GPT by e.g. overwriting autogpt/main.py which will be executed outside of the docker environment meant to sandbox custom python code execution the next time Auto-GPT is started. The issue has been patched in version 0.4.3. As a workaround, the risk introduced by this vulnerability can be remediated by running Auto-GPT in a virtual machine, or another environment in which damage to files or corruption of the program is not a critical problem.	7.5	More Details
CVE-2023-29298	Adobe ColdFusion versions 2018u16 (and earlier), 2021u6 (and earlier) and 2023.0.0.330468 (and earlier) are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to access the administration CFM and CFC endpoints. Exploitation of this issue does not require user interaction.	7.5	More Details
CVE-2023-2263	The Rockwell Automation Kinetix 5700 DC Bus Power Supply Series A is vulnerable to CIP fuzzing. The new ENIP connections cannot be established if impacted by this vulnerability, which prohibits operational capabilities of the device resulting in a denial-of-service attack.	7.5	More Details
CVE-2023-3596	Where this vulnerability exists in the Rockwell Automation 1756-EN4* Ethernet/IP communication products, it could allow a malicious user to cause a denial of service by asserting the target system through maliciously crafted CIP messages.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36835	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on QFX10000 Series allows a network based attacker to cause a Denial of Service (DoS). If a specific valid IP packet is received and that packet needs to be routed over a VXLAN tunnel, this will result in a PFE wedge condition due to which traffic gets impacted. As this is not a crash and restart scenario, this condition will persist until the system is rebooted to recover. This issue affects Juniper Networks Junos OS on QFX10000: 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S5; 21.3 versions prior to 21.3R3-S4; 21.4 versions prior to 21.4R3-S1; 22.1 versions prior to 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2.	7.5	More Details
CVE-2023-37474	Copyparty is a portable file server. Versions prior to 1.8.2 are subject to a path traversal vulnerability detected in the `.cpr` subfolder. The Path Traversal attack technique allows an attacker access to files, directories, and commands that reside outside the web document root directory. This issue has been addressed in commit `043e3c7d` which has been included in release 1.8.2. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.5	More Details
CVE-2023-38325	The cryptography package before 41.0.2 for Python mishandles SSH certificates that have critical options.	7.5	More Details
CVE-2022-41409	Integer overflow vulnerability in pcre2test before 10.41 allows attackers to cause a denial of service or other unspecified impacts via negative input.	7.5	More Details
CVE-2023-38286	Thymeleaf through 3.1.1.RELEASE, as used in spring-boot-admin (aka Spring Boot Admin) through 3.1.1 and other products, allows sandbox bypass via crafted HTML. This may be relevant for SSTI (Server Side Template Injection) and code execution in spring-boot-admin if MailNotifier is enabled and there is write access to environment variables via the UI.	7.5	More Details
CVE-2023-37599	An issue in issabel-pbx v.4.0.0-6 allows a remote attacker to obtain sensitive information via the modules directory	7.5	More Details
CVE-2022-47085	An issue was discovered in ostree before 2022.7 allows attackers to cause a denial of service or other unspecified impacts via the print_panic function in repo_checkout_filter.rs.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22435	Experion server may experience a DoS due to a stack overflow when handling a specially crafted message.	7.5	More Details
CVE-2023-35694	In DMPixelLogger_ProcessDmCommand of DMPixelLogger.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	7.5	More Details
CVE-2023-34123	Use of Hard-coded Cryptographic Key vulnerability in SonicWall GMS, SonicWall Analytics. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	7.5	More Details
CVE-2023-31819	An issue found in KEISEI STORE Co, Ltd. LIVRE KEISEI v.13.6.1 allows a remote attacker to gain access to sensitive information via the channel access token in the miniapp function.	7.5	More Details
CVE-2023-31825	An issue found in Inageya v.13.4.1 allows a remote attacker to gain access to sensitive information via the channel access token in the miniapp Inageya function.	7.5	More Details
CVE-2023-38197	An issue was discovered in Qt before 5.15.15, 6.x before 6.2.10, and 6.3.x through 6.5.x before 6.5.3. There are infinite loops in recursive entity expansion.	7.5	More Details
CVE-2023-37267	Umbraco is a ASP.NET CMS. Under rare conditions a restart of Umbraco can allow unauthorized users access to admin-level permissions. This vulnerability was patched in versions 10.6.1, 11.4.2 and 12.0.1.	7.5	More Details
CVE-2023-26597	Controller DoS due to buffer overflow in the handling of a specially crafted message received by the controller. See Honeywell Security Notification for recommendations on upgrading and versioning. See Honeywell Security Notification for recommendations on upgrading and versioning.	7.5	More Details
CVE-2023-25948	Server information leak of configuration data when an error is generated in response to a specially crafted message. See Honeywell Security Notification for recommendations on upgrading and versioning.	7.5	More Details
CVE-2023-24474	Experion server may experience a DoS due to a heap overflow which could occur when handling a specially crafted message	7.5	More Details
CVE-2023-31821	An issue found in ALBIS Co. ALBIS v.13.6.1 allows a remote attacker to gain access to sensitive information via the channel access token in the miniapp ALBIS function.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31822	An issue found in Entetsu Store v.13.4.1 allows a remote attacker to gain access to sensitive information via the channel access token in the miniapp Entetsu Store function.	7.5	More Details
CVE-2023-31823	An issue found in Marui Co Marui Official app v.13.6.1 allows a remote attacker to gain access to sensitive information via the channel access token in the miniapp Marui Official Store function.	7.5	More Details
CVE-2023-34133	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in SonicWall GMS and Analytics allows an unauthenticated attacker to extract sensitive information from the application database. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	7.5	More Details
CVE-2023-31824	An issue found in DERICIA Co. Ltd, DELICIA v.13.6.1 allows a remote attacker to gain access to sensitive information via the channel access token in the miniapp DELICIA function.	7.5	More Details
CVE-2023-22047	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.59 and 8.60. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2023-35945	Envoy is a cloud-native high-performance edge/middle/service proxy. Envoy's HTTP/2 codec may leak a header map and bookkeeping structures upon receiving `RST_STREAM` immediately followed by the `GOAWAY` frames from an upstream server. In nghttp2, cleanup of pending requests due to receipt of the `GOAWAY` frame skips de-allocation of the bookkeeping structure and pending compressed header. The error return [code path] is taken if connection is already marked for not sending more requests due to `GOAWAY` frame. The clean-up code is right after the return statement, causing memory leak. Denial of service through memory exhaustion. This vulnerability was patched in versions(s) 1.26.3, 1.25.8, 1.24.9, 1.23.11.	7.5	More Details
CVE-2023-30906	The vulnerability could be locally exploited to allow escalation of privilege.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2913	An executable used in Rockwell Automation ThinManager ThinServer can be configured to enable an API feature in the HTTPS Server Settings. This feature is disabled by default. When the API is enabled and handling requests, a path traversal vulnerability exists that allows a remote actor to leverage the privileges of the server's file system and read arbitrary files stored in it. A malicious user could exploit this vulnerability by executing a path that contains manipulating variables.	7.5	More Details
CVE-2023-37788	goproxy v1.1 was discovered to contain an issue which can lead to a Denial of service (DoS) via unspecified vectors.	7.5	More Details
CVE-2023-37758	D-LINK DIR-815 v1.01 was discovered to contain a buffer overflow via the component /web/captcha.cgi.	7.5	More Details
CVE-2020-20021	An issue discovered in MikroTik Router v6.46.3 and earlier allows attacker to cause denial of service via misconfiguration in the SSH daemon.	7.5	More Details
CVE-2023-33871	Iagona ScrutisWeb versions 2.1.37 and prior are vulnerable to a directory traversal vulnerability that could allow an unauthenticated user to directly access any file outside the webroot.	7.5	More Details
CVE-2023-30383	TP-LINK Archer C50v2 Archer C50(US)_V2_160801, TP-LINK Archer C20v1 Archer_C20_V1_150707, and TP-LINK Archer C2v1 Archer_C2_US__V1_170228 were discovered to contain a buffer overflow which may lead to a Denial of Service (DoS) when parsing crafted data.	7.5	More Details
CVE-2023-38405	On Crestron 3-Series Control Systems before 1.8001.0187, crafting and sending a specific BACnet packet can cause a crash.	7.5	More Details
CVE-2023-38337	rswag before 2.10.1 allows remote attackers to read arbitrary JSON and YAML files via directory traversal, because rswag-api can expose a file that is not the OpenAPI (or Swagger) specification file of a project.	7.5	More Details
CVE-2023-34669	TOTOLINK CP300+ V5.2cu.7594 contains a Denial of Service vulnerability in function RebootSystem of the file lib/cste_modules/system which can reboot the system.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37475	Hamba avro is a go lang encoder/decoder implementation of the avro codec specification. In affected versions a well-crafted string passed to avro's `github.com/hamba/avro/v2.Unmarshal()` can throw a `fatal error: runtime: out of memory` which is unrecoverable and can cause denial of service of the consumer of avro. The root cause of the issue is that avro uses part of the input to `Unmarshal()` to determine the size when creating a new slice and hence an attacker may consume arbitrary amounts of memory which in turn may cause the application to crash. This issue has been addressed in commit `b4a402f4` which has been included in release version `2.13.0`. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.5	More Details
CVE-2023-2959	Authentication Bypass by Primary Weakness vulnerability in Oliva Expertise Oliva Expertise EKS allows Collect Data as Provided by Users.This issue affects Oliva Expertise EKS: before 1.2.	7.5	More Details
CVE-2023-38257	Iagona ScrutisWeb versions 2.1.37 and prior are vulnerable to an insecure direct object reference vulnerability that could allow an unauthenticated user to view profile information, including user login names and encrypted passwords.	7.5	More Details
CVE-2023-38379	The web interface on the RIGOL MSO5000 digital oscilloscope with firmware 00.01.03.00.03 allows remote attackers to change the admin password via a zero-length pass0 to the webcontrol changepwd.cgi application, i.e., the entered password only needs to match the first zero characters of the saved password.	7.5	More Details
CVE-2023-38403	iperf3 before 3.14 allows peers to cause an integer overflow and heap corruption via a crafted length field.	7.5	More Details
CVE-2021-37386	Furukawa Electric LatAm 423-41W/AC before v1.1.4 and LD421-21W before v1.3.3 were discovered to contain an HTML injection vulnerability via the serial number update function.	7.5	More Details
CVE-2023-31998	A heap overflow vulnerability found in EdgeRouters and Aircubes allows a malicious actor to interrupt UPnP service to said devices.	7.5	More Details
CVE-2023-38434	xHTTP 72f812d has a double free in close_connection in xhttp.c via a malformed HTTP request method.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3525	The Getnet Argentina para Woocommerce plugin for WordPress is vulnerable to authorization bypass due to missing validation on the 'webhook' function in versions up to, and including, 0.0.4. This makes it possible for unauthenticated attackers to set their payment status to 'APPROVED' without payment.	7.5	More Details
CVE-2023-3714	The ProfileGrid plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'edit_group' handler in versions up to, and including, 5.5.2. This makes it possible for authenticated attackers, with group ownership, to update group options, including the 'associate_role' parameter, which defines the member's role. This issue was partially patched in version 5.5.2 preventing privilege escalation, however, it was fully patched in 5.5.3.	7.5	More Details
CVE-2023-3743	Ap Page Builder, in versions lower than 1.7.8.2, could allow a remote attacker to send a specially crafted SQL query to the product_one_img parameter to retrieve the information stored in the database.	7.5	More Details
CVE-2023-20185	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability.	7.4	More Details
CVE-2022-4146	Expression Language Injection vulnerability in Hitachi Replication Manager on Windows, Linux, Solaris allows Code Injection.This issue affects Hitachi Replication Manager: before 8.8.5-02.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34035	Spring Security versions 5.8 prior to 5.8.5, 6.0 prior to 6.0.5, and 6.1 prior to 6.1.2 could be susceptible to authorization rule misconfiguration if the application uses requestMatchers(String) and multiple servlets, one of them being Spring MVC's DispatcherServlet. (DispatcherServlet is a Spring MVC component that maps HTTP endpoints to methods on @Controller-annotated classes.) Specifically, an application is vulnerable when all of the following are true: * Spring MVC is on the classpath * Spring Security is securing more than one servlet in a single application (one of them being Spring MVC's DispatcherServlet) * The application uses requestMatchers(String) to refer to endpoints that are not Spring MVC endpoints An application is not vulnerable if any of the following is true: * The application does not have Spring MVC on the classpath * The application secures no servlets other than Spring MVC's DispatcherServlet * The application uses requestMatchers(String) only for Spring MVC endpoints	7.3	More Details
CVE-2023-3643	A vulnerability was found in Boss Mini 1.4.0 Build 6221. It has been classified as critical. This affects an unknown part of the file boss/servlet/document. The manipulation of the argument path leads to file inclusion. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-233889 was assigned to this vulnerability.	7.3	More Details
CVE-2023-3693	A vulnerability classified as critical was found in SourceCodester Life Insurance Management System 1.0. This vulnerability affects unknown code of the file login.php. The manipulation of the argument username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-234244.	7.3	More Details
CVE-2023-21251	In onCreate of ConfirmDialog.java, there is a possible way to connect to VNP bypassing user's consent due to improper input validation. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.	7.3	More Details
CVE-2023-3158	The Mail Control plugin for WordPress is vulnerable to Stored Cross-Site Scripting via an email subject in versions up to, and including, 0.2.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3166	The Lana Email Logger plugin for WordPress is vulnerable to Stored Cross-Site Scripting via an email subject in versions up to, and including, Lana Email Logger due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2023-3135	The Mailtree Log Mail plugin for WordPress is vulnerable to Stored Cross-Site Scripting via an email subject in versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2023-3081	The WP Mail Logging plugin for WordPress is vulnerable to Stored Cross-Site Scripting via email contents in versions up to, and including, 1.11.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Note: An incomplete fix was released in 1.11.1.	7.2	More Details
CVE-2023-3080	The WP Mail Catcher plugin for WordPress is vulnerable to Stored Cross-Site Scripting via an email subject in versions up to, and including, 2.1.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2023-3168	The WP Reroute Email plugin for WordPress is vulnerable to Stored Cross-Site Scripting via an email subject in versions up to, and including, 1.4.9 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2023-37477	1Panel is an open source Linux server operation and maintenance management panel. An OS command injection vulnerability exists in 1Panel firewall functionality. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability. 1Panel firewall functionality `/hosts/firewall/ip` endpoint read user input without validation, the attacker extends the default functionality of the application, which execute system commands. An attacker can execute arbitrary code on the target system, which can lead to a complete compromise of the system. This issue has been addressed in commit `e17b80cff49` which is included in release version `1.4.3`. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3093	The YaySMTP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via email contents in versions up to, and including, 2.4.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2023-35691	there is a possible out of bounds read due to a missing bounds check. This could lead to remote denial of service with System execution privileges needed. User interaction is not needed for exploitation.	7.2	More Details
CVE-2023-38404	The XPRTLD web application in Veritas InfoScale Operations Manager (VIOM) before 8.0.0.410 allows an authenticated attacker to upload all types of files to the server. An authenticated attacker can then execute the malicious file to perform command execution on the remote server.	7.2	More Details
CVE-2023-3459	The Export and Import Users and Customers plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'hf_update_customer' function called via an AJAX action in versions up to, and including, 2.4.1. This makes it possible for authenticated attackers, with shop manager-level permissions to change user passwords and potentially take over administrator accounts.	7.2	More Details
CVE-2023-37897	Grav is a file-based Web-platform built in PHP. Grav is subject to a server side template injection (SSTI) vulnerability. The fix for another SSTI vulnerability using `|map`, `|filter` and `|reduce` twigs implemented in the commit `71bbed1` introduces bypass of the denylist due to incorrect return value from `isDangerousFunction()`, which allows to execute the payload prepending double backslash (`\\`). The `isDangerousFunction()` check in version 1.7.42 and onwards retuns `false` value instead of `true` when the `\` symbol is found in the `$name`. This vulnerability can be exploited if the attacker has access to: 1. an Administrator account, or 2. a non-administrator, user account that has Admin panel access and Create/Update page permissions. A fix for this vulnerability has been introduced in commit `b4c6210` and is included in release version `1.7.42.2`. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.2	More Details
CVE-2023-3122	The GD Mail Queue plugin for WordPress is vulnerable to Stored Cross-Site Scripting via email contents in versions up to, and including, 3.9.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3167	The Mail Queue plugin for WordPress is vulnerable to Stored Cross-Site Scripting via an email subject in versions up to, and including, 1.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2023-3668	Improper Encoding or Escaping of Output in GitHub repository froxlor/froxlor prior to 2.0.21.	7.2	More Details
CVE-2023-3088	The WP Mail Log plugin for WordPress is vulnerable to Stored Cross-Site Scripting via email contents in versions up to, and including, 1.1.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2023-3082	The Post SMTP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via email contents in versions up to, and including, 2.5.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2023-3087	The FluentSMTP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via an email subject in versions up to, and including, 2.2.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2023-3692	Unrestricted Upload of File with Dangerous Type in GitHub repository admidio/admidio prior to 4.2.10.	7.2	More Details
CVE-2023-3023	The WP EasyCart plugin for WordPress is vulnerable to time-based SQL Injection via the ‘orderby’ parameter in versions up to, and including, 5.4.10 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level or above permissions, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.2	More Details
CVE-2023-3673	SQL Injection in GitHub repository pimcore/pimcore prior to 10.5.24.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3092	The SMTP Mail plugin for WordPress is vulnerable to Stored Cross-Site Scripting via an email subject in versions up to, and including, 1.2.16 due to insufficient input sanitization and output escaping when the 'Save Data SendMail' feature is enabled. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2023-36384	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in CodePeople Booking Calendar Contact Form plugin <= 1.2.40 versions.	7.1	More Details
CVE-2023-34458	mx-chain-go is the official implementation of the MultiversX blockchain protocol, written in golang. When executing a relayed transaction, if the inner transaction failed, it would have increased the inner transaction's sender account nonce. This could have contributed to a limited DoS attack on a targeted account. The fix is a breaking change so a new flag `RelayedNonceFixEnableEpoch` was needed. This was a strict processing issue while validating blocks on a chain. This vulnerability has been patched in version 1.4.17.	7.1	More Details
CVE-2023-2268	Plane version 0.7.1 allows an unauthenticated attacker to view all stored server files of all users.	7.1	More Details
CVE-2023-30791	Plane version 0.7.1-dev allows an attacker to change the avatar of his profile, which allows uploading files with HTML extension that interprets both HTML and JavaScript.	7.1	More Details
CVE-2023-37965	A missing permission check in Jenkins ElasticBox CI Plugin 5.0.1 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	7.1	More Details
CVE-2023-33312	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in wppal Easy Captcha plugin <= 1.0 versions.	7.1	More Details
CVE-2023-32965	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in CRUDLab Jazz Popups plugin <= 1.8.7 versions.	7.1	More Details
CVE-2023-37949	A missing permission check in Jenkins Orka by MacStadium Plugin 1.33 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-23909	Heap-based buffer over-read in function png_convert_4 in file pngex.cc in AdvanceMAME through 2.1.	7.1	More Details
CVE-2022-24834	Redis is an in-memory database that persists on disk. A specially crafted Lua script executing in Redis can trigger a heap overflow in the cjson library, and result with heap corruption and potentially remote code execution. The problem exists in all versions of Redis with Lua scripting support, starting from 2.6, and affects only authenticated and authorized users. The problem is fixed in versions 7.0.12, 6.2.13, and 6.0.20.	7.0	More Details
CVE-2023-30564	Alaris Systems Manager does not perform input validation during the Device Import Function.	6.9	More Details
CVE-2023-37278	GLPI is a Free Asset and IT Management Software package, Data center management, ITIL Service Desk, licenses tracking and software auditing. An administrator can trigger SQL injection via dashboards administration. This vulnerability has been patched in version 10.0.9.	6.8	More Details
CVE-2023-35818	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code.	6.8	More Details
CVE-2023-37199	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists that could cause remote code execution when an admin user on DCE tampers with backups which are then manually restored.	6.8	More Details
CVE-2023-36473	Discourse is an open source discussion platform. A CSP (Content Security Policy) nonce reuse vulnerability could allow XSS attacks to bypass CSP protection. There are no known XSS vectors at the moment, but should one be discovered, this vulnerability would allow the XSS attack to completely bypass CSP. The vulnerability is patched in the latest tests-passed, beta and stable branches.	6.8	More Details
CVE-2023-37198	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists that could cause remote code execution when an admin user on DCE uploads or tampers with install packages.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30560	The configuration from the PCU can be modified without authentication using physical connection to the PCU.	6.8	More Details
CVE-2023-3527	A CSV injection vulnerability was found in the Avaya Call Management System (CMS) Supervisor web application which allows a user with administrative privileges to input crafted data which, when exported to a CSV file, may attempt arbitrary command execution on the system used to open the file by a spreadsheet software such as Microsoft Excel.	6.8	More Details
CVE-2023-35693	In incfs_kill_sb of fs/incfs/vfs.c, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	6.7	More Details
CVE-2022-42045	Certain Zemana products are vulnerable to Arbitrary code injection. This affects Watchdog Anti-Malware 4.1.422 and Zemana AntiMalware 3.2.28.	6.7	More Details
CVE-2023-35012	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 with a Federated configuration is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. A local user with SYSADM privileges could overflow the buffer and execute arbitrary code on the system. IBM X-Force ID: 257763.	6.7	More Details
CVE-2023-30562	A GRE dataset file within Systems Manager can be tampered with and distributed to PCUs.	6.7	More Details
CVE-2021-43072	A buffer copy without checking size of input ('classic buffer overflow') in Fortinet FortiAnalyzer version 7.0.2 and below, version 6.4.7 and below, version 6.2.9 and below, version 6.0.11 and below, version 5.6.11 and below, FortiManager version 7.0.2 and below, version 6.4.7 and below, version 6.2.9 and below, version 6.0.11 and below, version 5.6.11 and below, FortiOS version 7.0.0 through 7.0.4, 6.4.0 through 6.4.8, 6.2.0 through 6.2.10, 6.0.x and FortiProxy version 7.0.0 through 7.0.3, 2.0.0 through 2.0.8, 1.2.x, 1.1.x and 1.0.x allows attacker to execute unauthorized code or commands via crafted CLI `execute restore image` and `execute certificate remote` operations with the tFTP protocol.	6.7	More Details
CVE-2023-21400	In multiple functions of io_uring.c, there is a possible kernel memory corruption due to improper locking. This could lead to local escalation of privilege in the kernel with System execution privileges needed. User interaction is not needed for exploitation.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36695	Incorrect Default Permissions vulnerability in Hitachi Device Manager on Linux (Device Manager Server component), Hitachi Tiered Storage Manager on Linux, Hitachi Replication Manager on Linux, Hitachi Tuning Manager on Linux (Hitachi Tuning Manager server, Hitachi Tuning Manager - Agent for RAID, Hitachi Tuning Manager - Agent for NAS components), Hitachi Compute Systems Manager on Linux allows File Manipulation.This issue affects Hitachi Device Manager: before 8.8.5-02; Hitachi Tiered Storage Manager: before 8.8.5-02; Hitachi Replication Manager: before 8.8.5-02; Hitachi Tuning Manager: before 8.8.5-02; Hitachi Compute Systems Manager: before 8.8.3-08.	6.6	More Details
CVE-2023-3106	A NULL pointer dereference vulnerability was found in netlink_dump. This issue can occur when the Netlink socket receives the message(sendmsg) for the XFRM_MSG_GETSA, XFRM_MSG_GETPOLICY type message, and the DUMP flag is set and can cause a denial of service or possibly another unspecified impact. Due to the nature of the flaw, privilege escalation cannot be fully ruled out, although it is unlikely.	6.6	More Details
CVE-2023-33768	Incorrect signature verification of the firmware during the Device Firmware Update process of Belkin Wemo Smart Plug WSP080 v1.2 allows attackers to cause a Denial of Service (DoS) via a crafted firmware file.	6.5	More Details
CVE-2023-35908	Apache Airflow, versions before 2.6.3, is affected by a vulnerability that allows unauthorized read access to a DAG through the URL. It is recommended to upgrade to a version that is not affected	6.5	More Details
CVE-2023-2190	An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.10 before 15.11.10, all versions starting from 16.0 before 16.0.6, all versions starting from 16.1 before 16.1.1. It may be possible for users to view new commits to private projects in a fork created while the project was public.	6.5	More Details
CVE-2023-22040	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H).	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37955	A cross-site request forgery (CSRF) vulnerability in Jenkins Test Results Aggregator Plugin 1.2.13 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials.	6.5	More Details
CVE-2023-37837	libjpeg commit db33a6e was discovered to contain a heap buffer overflow via LineBitmapRequester::EncodeRegion at linebitmaprequester.cpp. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted file.	6.5	More Details
CVE-2023-37953	A missing permission check in Jenkins mabl Plugin 0.0.46 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	6.5	More Details
CVE-2023-37952	A cross-site request forgery (CSRF) vulnerability in Jenkins mabl Plugin 0.0.46 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	6.5	More Details
CVE-2023-38068	In JetBrains YouTrack before 2023.1.16597 captcha was not properly validated for Helpdesk forms	6.5	More Details
CVE-2023-36848	An Improper Handling of Undefined Values vulnerability in the periodic packet management daemon (PPMD) of Juniper Networks Junos OS on MX Series(except MPC10, MPC11 and LC9600) allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When a malformed CFM packet is received, it leads to an FPC crash. Continued receipt of these packets causes a sustained denial of service. This vulnerability occurs only when CFM has been configured on the interface. This issue affects Juniper Networks Junos OS: versions prior to 19.1R3-S10 on MX Series; 19.2 versions prior to 19.2R3-S7 on MX Series; 19.3 versions prior to 19.3R3-S8 on MX Series; 19.4 versions prior to 19.4R3-S12 on MX Series; 20.1 version 20.1R1 and later versions on MX Series; 20.2 versions prior to 20.2R3-S8 on MX Series; 20.3 version 20.3R1 and later versions on MX Series; 20.4 versions prior to 20.4R3-S7 on MX Series; 21.1 versions prior to 21.1R3-S5 on MX Series; 21.2 versions prior to 21.2R3-S5 on MX Series; 21.3 versions prior to 21.3R3-S4 on MX Series; 21.4 versions prior to 21.4R3-S4 on MX Series; 22.1 versions prior to 22.1R3-S3 on MX Series; 22.2 versions prior to 22.2R3-S1 on MX Series; 22.3 versions prior to 22.3R3 on MX Series; 22.4 versions prior to 22.4R1-S2, 22.4R2 on MX Series.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36849	An Improper Check or Handling of Exceptional Conditions vulnerability in the Layer-2 control protocols daemon (l2cpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When a malformed LLDP packet is received, l2cpd will crash and restart. The impact of the l2cpd crash is reinitialization of STP protocols (RSTP, MSTP or VSTP), and MVRP and ERP. Also, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. Continued receipt of such packets will lead to a sustained Denial of Service. This issue affects: Juniper Networks Junos OS 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S3; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R2. Juniper Networks Junos OS Evolved 21.4-EVO versions prior to 21.4R3-S2-EVO; 22.1-EVO versions prior to 22.1R3-S3-EVO; 22.2-EVO versions prior to 22.2R2-S1-EVO, 22.2R3-EVO; 22.3-EVO versions prior to 22.3R2-EVO.	6.5	More Details
CVE-2023-36850	An Improper Validation of Specified Index, Position, or Offset in Input vulnerability in the Connectivity Fault Management(CFM) module of Juniper Networks Junos OS on MX Series(except MPC10, MPC11 and LC9600) allows an adjacent attacker on the local broadcast domain to cause a Denial of Service(DoS). Upon receiving a malformed CFM packet, the MPC crashes. Continued receipt of these packets causes a sustained denial of service. This issue can only be triggered when CFM hasn't been configured. This issue affects: Juniper Networks Junos OS All versions prior to 19.1R3-S10 on MX Series; 19.2 versions prior to 19.2R3-S7 on MX Series; 19.3 versions prior to 19.3R3-S8 on MX Series; 19.4 versions prior to 19.4R3-S12 on MX Series; 20.1 version 20.1R1 and later versions on MX Series; 20.2 versions prior to 20.2R3-S7 on MX Series; 20.3 version 20.3R1 and later versions on MX Series; 20.4 versions prior to 20.4R3-S7 on MX Series; 21.1 versions prior to 21.1R3-S5 on MX Series; 21.2 versions prior to 21.2R3-S4 on MX Series; 21.3 versions prior to 21.3R3-S4 on MX Series; 21.4 versions prior to 21.4R3-S3 on MX Series; 22.1 versions prior to 22.1R3-S2 on MX Series; 22.2 versions prior to 22.2R3 on MX Series; 22.3 versions prior to 22.3R2, 22.3R3 on MX Series; 22.4 versions prior to 22.4R2 on MX Series.	6.5	More Details
CVE-2023-36514	Cross-Site Request Forgery (CSRF) vulnerability in WooCommerce Shipping Multiple Addresses plugin <= 3.8.5 versions.	6.5	More Details
CVE-2023-36543	Apache Airflow, versions before 2.6.3, has a vulnerability where an authenticated user can use crafted input to make the current request hang. It is recommended to upgrade to a version that is not affected	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34134	Exposure of sensitive information to an unauthorized actor vulnerability in SonicWall GMS and Analytics allows authenticated attacker to read administrator password hash via a web service call. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	6.5	More Details
CVE-2023-34135	Path Traversal vulnerability in SonicWall GMS and Analytics allows a remote authenticated attacker to read arbitrary files from the underlying file system via web service. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	6.5	More Details
CVE-2023-37563	ELECOM wireless LAN routers are vulnerable to sensitive information exposure, which allows a network-adjacent unauthorized attacker to obtain sensitive information. Affected products and versions are as follows: WRC-1167GHBK-S v1.03 and earlier, WRC-1167GEBK-S v1.03 and earlier, WRC-1167FEBK-S v1.04 and earlier, WRC-1167GHBK3-A v1.24 and earlier, WRC-1167FEBK-A v1.18 and earlier, WRC-F1167ACF2 all versions, WRC-600GHBK-A all versions, WRC-733FEBK2-A all versions, WRC-1467GHBK-A all versions, WRC-1467GHBK-S all versions, WRC-1900GHBK-A all versions, and WRC-1900GHBK-S all versions.	6.5	More Details
CVE-2023-37951	Jenkins mabl Plugin 0.0.46 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.	6.5	More Details
CVE-2023-37849	A DLL hijacking vulnerability in Panda Security VPN for Windows prior to version v15.14.8 allows attackers to execute arbitrary code via placing a crafted DLL file in the same directory as PANDAVPN.exe.	6.5	More Details
CVE-2023-37942	Jenkins External Monitor Job Type Plugin 206.v9a_94ff0b_4a_10 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	6.5	More Details
CVE-2023-3011	The ARMember plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.0.5. This is due to missing or incorrect nonce validation on the arm_check_user_cap function. This makes it possible for unauthenticated attackers to perform multiple unauthorized actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.5	More Details
CVE-2021-32256	An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22037	Vulnerability in the Oracle Web Applications Desktop Integrator product of Oracle E-Business Suite (component: MS Excel Specific). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Web Applications Desktop Integrator. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Web Applications Desktop Integrator, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Web Applications Desktop Integrator accessible data as well as unauthorized read access to a subset of Oracle Web Applications Desktop Integrator accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Web Applications Desktop Integrator. CVSS 3.1 Base Score 6.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L).	6.5	More Details
CVE-2023-36818	Discourse is an open source discussion platform. In affected versions a request to create or update custom sidebar section can cause a denial of service. This issue has been patched in commit `52b003d915`. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.5	More Details
CVE-2023-34125	Path Traversal vulnerability in GMS and Analytics allows an authenticated attacker to read arbitrary files from the underlying filesystem with root privileges. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	6.5	More Details
CVE-2023-37960	Jenkins MathWorks Polyspace Plugin 1.0.5 and earlier allows attackers with Item/Configure permission to send emails with arbitrary files from the Jenkins controller file systems.	6.5	More Details
CVE-2023-35833	An issue was discovered in YSoft SAFEQ 6 Server before 6.0.82. When modifying the URL of the LDAP server configuration from LDAPS to LDAP, the system does not require the password to be (re)entered. This results in exposing cleartext credentials when connecting to a rogue LDAP server. NOTE: the vendor originally reported this as a security issue but then reconsidered because of the requirement for Admin access in order to change the configuration.	6.5	More Details
CVE-2023-34005	Cross-Site Request Forgery (CSRF) vulnerability in Etoile Web Design Front End Users plugin <= 3.2.24 versions.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22022	Vulnerability in the Oracle Health Sciences Sciences Data Management Workbench product of Oracle Health Sciences Applications (component: Blinding Functionality). Supported versions that are affected are 3.1.0.2, 3.1.1.3 and 3.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences Sciences Data Management Workbench. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Health Sciences Sciences Data Management Workbench accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2023-36833	A Use After Free vulnerability in the packet forwarding engine (PFE) of Juniper Networks Junos OS Evolved on PTX10001-36MR, and PTX10004, PTX10008, PTX10016 with LC1201/1202 allows an adjacent, unauthenticated attacker to cause a Denial of Service (DoS). The process 'aftman-bt' will crash after multiple flaps on a multicast-only fast reroute (MoFRR) enabled interface. This will cause the respective FPC to stop forwarding traffic and it needs to be rebooted to restore the service. An indication that the system experienced this issue is the following log message: <date> <hostname> evo-aftmand-bt[<pid>]: [Error] jexpr_fdb: sanity check failed, ... , app_name L3 Mcast Routes This issue affects Juniper Networks Junos OS Evolved on PTX10001-36MR, PTX10004, PTX10008, PTX10016 with LC1201/1202: 21.2 version 21.2R1-EVO and later versions; 21.3 version 21.3R1-EVO and later versions; 21.4 versions prior to 21.4R3-S3-EVO; 22.1 version 22.1R1-EVO and later versions; 22.2 versions prior to 22.2R3-S2-EVO; 22.3 versions prior to 22.3R3-EVO; 22.4 versions prior to 22.4R1-S2-EVO, 22.4R2-EVO.	6.5	More Details
CVE-2023-37944	A missing permission check in Jenkins Datadog Plugin 5.4.1 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	6.5	More Details
CVE-2022-46651	Apache Airflow, versions before 2.6.3, is affected by a vulnerability that allows an unauthorized actor to gain access to sensitive information in Connection edit view. This vulnerability is considered low since it requires someone with access to Connection resources specifically updating the connection to exploit it. Users should upgrade to version 2.6.3 or later which has removed the vulnerability.	6.5	More Details
CVE-2023-3618	A flaw was found in libtiff. A specially crafted tiff file can lead to a segmentation fault due to a buffer overflow in the Fax3Encode function in libtiff/tif_fax3.c, resulting in a denial of service.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36834	An Incomplete Internal State Distinction vulnerability in the packet forwarding engine (PFE) of Juniper Networks Junos OS on SRX 4600 and SRX 5000 Series allows an adjacent attacker to cause a Denial of Service (DoS). If an SRX is configured in L2 transparent mode the receipt of a specific genuine packet can cause a single Packet Processing Engines (PPE) component of the PFE to run into a loop, which in turn will render the PPE unavailable. Each packet will cause one PPE to get into a loop, leading to a gradual performance degradation until all PPEs are unavailable and all traffic processing stops. To recover the affected FPC need to be restarted. This issue affects Juniper Networks Junos OS on SRX 4600 and SRX 5000 Series: 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S7; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S1; 22.1 versions prior to 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S1, 22.3R2.	6.5	More Details
CVE-2023-21994	Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator App). Supported versions that are affected are Prior to 11.1.2.3.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Mobile Security Suite executes to compromise Oracle Mobile Security Suite. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Mobile Security Suite accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2023-37456	The session restore helper crashed whenever there was no parameter sent to the message handler. This vulnerability affects Firefox for iOS < 115.	6.5	More Details
CVE-2023-34140	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30858	An issue was discovered in ngiflib 0.4. There is SEGV in SDL_LoadAnimatedGif when use SDLaffgif. poc : ./SDLaffgif CA_file2_0	6.5	More Details
CVE-2023-37769	stress-test master commit e4c878 was discovered to contain a FPE vulnerability via the component combine_inner at /pixman-combine-float.c.	6.5	More Details
CVE-2023-37959	A missing permission check in Jenkins Sumologic Publisher Plugin 2.2.1 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL.	6.5	More Details
CVE-2023-37781	An issue in the emqx_sn plugin of EMQX v4.3.8 allows attackers to execute a directory traversal via uploading a crafted .txt file.	6.5	More Details
CVE-2023-22887	Apache Airflow, versions before 2.6.3, is affected by a vulnerability that allows an attacker to perform unauthorized file access outside the intended directory structure by manipulating the run_id parameter. This vulnerability is considered low since it requires an authenticated user to exploit it. It is recommended to upgrade to a version that is not affected	6.5	More Details
CVE-2023-37956	A missing permission check in Jenkins Test Results Aggregator Plugin 1.2.13 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials.	6.5	More Details
CVE-2023-22888	Apache Airflow, versions before 2.6.3, is affected by a vulnerability that allows an attacker to cause a service disruption by manipulating the run_id parameter. This vulnerability is considered low since it requires an authenticated user to exploit it. It is recommended to upgrade to a version that is not affected	6.5	More Details
CVE-2023-37836	libjpeg commit db33a6e was discovered to contain a reachable assertion via BitMapHook::BitMapHook at bitmaphook.cpp. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted file.	6.5	More Details
CVE-2023-37463	cmark-gfm is an extended version of the C reference implementation of CommonMark, a rationalized version of Markdown syntax with a spec. Three polynomial time complexity issues in cmark-gfm may lead to unbounded resource exhaustion and subsequent denial of service. These vulnerabilities have been patched in 0.29.0.gfm.12.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2433	The YARPP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'className' parameter in versions up to, and including, 5.30.3 due to insufficient input sanitization and output escaping. This makes it possible for contributor-level attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-37268	Warpgate is an SSH, HTTPS and MySQL bastion host for Linux that doesn't need special client apps. When logging in as a user with SSO enabled an attacker may authenticate as an other user. Any user account which does not have a second factor enabled could be compromised. This issue has been addressed in commit `8173f6512a` and in releases starting with version 0.7.3. Users are advised to upgrade. Users unable to upgrade should require their users to use a second factor in authentication.	6.4	More Details
CVE-2023-2082	The "Buy Me a Coffee – Button and Widget Plugin" plugin for WordPress is vulnerable to Cross-Site Scripting in versions up to, and including, 3.6 due to insufficient sanitization and escaping on the 'text value set via the bmc_post_reception action. This makes it possible for authenticated attackers, with subscriber-level permissions, and above to inject arbitrary web scripts into pages that execute whenever a victim accesses a page with the injected scripts.	6.4	More Details
CVE-2023-3689	A vulnerability classified as critical was found in Bylancer QuickQR 6.3.7. Affected by this vulnerability is an unknown functionality of the file /blog of the component GET Parameter Handler. The manipulation of the argument s leads to sql injection. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-234235. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-3687	A vulnerability was found in Bylancer QuickVCard 2.1. It has been rated as critical. This issue affects some unknown processing of the file /blog of the component GET Parameter Handler. The manipulation of the argument s leads to sql injection. The attack may be initiated remotely. The identifier VDB-234233 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-3700	Authorization Bypass Through User-Controlled Key in GitHub repository alextselegidis/easyappointments prior to 1.5.0.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3679	A vulnerability was found in SourceCodester Lost and Found Information System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /classes/Master.php?f=save_inquiry of the component HTTP POST Request Handler. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The identifier of this vulnerability is VDB-234224.	6.3	More Details
CVE-2023-3644	A vulnerability was found in SourceCodester Service Provider Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /classes/Master.php?f=save_inquiry. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. VDB-233890 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-3680	A vulnerability classified as critical has been found in SourceCodester Lost and Found Information System 1.0. This affects an unknown part of the file /classes/Master.php?f=save_item of the component HTTP POST Request Handler. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The identifier VDB-234225 was assigned to this vulnerability.	6.3	More Details
CVE-2023-3682	A vulnerability, which was classified as critical, was found in Nesote Inout Blockchain EasyPayments 1.0. Affected is an unknown function of the file /index.php/payment/getcoinaddress of the component POST Parameter Handler. The manipulation of the argument coinid leads to sql injection. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-234228. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-3695	A vulnerability classified as critical has been found in Campcodes Beauty Salon Management System 1.0. Affected is an unknown function of the file add-product.php. The manipulation of the argument category leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-234252.	6.3	More Details
CVE-2023-3661	A vulnerability was found in SourceCodester AC Repair and Services System 1.0. It has been classified as critical. This affects an unknown part of the file /classes/Master.php?f=save_inquiry. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-234015.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3694	A vulnerability, which was classified as critical, has been found in SourceCodester House Rental and Property Listing 1.0. This issue affects some unknown processing of the file index.php. The manipulation of the argument keywords/location leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-234245 was assigned to this vulnerability.	6.3	More Details
CVE-2023-3690	A vulnerability, which was classified as critical, has been found in Bylancer QuickOrder 6.3.7. Affected by this issue is some unknown functionality of the file /blog of the component GET Parameter Handler. The manipulation of the argument s leads to sql injection. The attack may be launched remotely. The identifier of this vulnerability is VDB-234236. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-3688	A vulnerability classified as critical has been found in Bylancer QuickJob 6.1. Affected is an unknown function of the component GET Parameter Handler. The manipulation of the argument keywords/gender leads to sql injection. It is possible to launch the attack remotely. VDB-234234 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-3658	A vulnerability, which was classified as critical, was found in SourceCodester AC Repair and Services System 1.0. Affected is an unknown function of the file Master.php?f=delete_book of the component HTTP POST Request Handler. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-234012.	6.3	More Details
CVE-2023-3678	A vulnerability was found in SourceCodester AC Repair and Services System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /classes/Master.php?f=delete_inquiry of the component HTTP POST Request Handler. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-234223.	6.3	More Details
CVE-2015-10122	A vulnerability was found in wp-donate Plugin up to 1.4 on WordPress. It has been classified as critical. This affects an unknown part of the file includes/donate-display.php. The manipulation leads to sql injection. It is possible to initiate the attack remotely. Upgrading to version 1.5 is able to address this issue. The identifier of the patch is 019114cb788d954c5d1b36d6c62418619e93a757. It is recommended to upgrade the affected component. The identifier VDB-234249 was assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29457	Reflected XSS attacks, occur when a malicious script is reflected off a web application to the victim's browser. The script can be activated through Action form fields, which can be sent as request to a website with a vulnerability that enables execution of malicious scripts.	6.3	More Details
CVE-2023-3686	A vulnerability was found in Bylancer QuickAI OpenAI 3.8.1. It has been declared as critical. This vulnerability affects unknown code of the file /blog of the component GET Parameter Handler. The manipulation of the argument s leads to sql injection. The attack can be initiated remotely. The identifier of this vulnerability is VDB-234232. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-36888	Microsoft Edge for Android (Chromium-based) Tampering Vulnerability	6.3	More Details
CVE-2023-3657	A vulnerability, which was classified as critical, has been found in SourceCodester AC Repair and Services System 1.0. This issue affects some unknown processing of the file Master.php?f=save_book of the component HTTP POST Request Handler. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-234011.	6.3	More Details
CVE-2023-37272	JS7 is an Open Source Job Scheduler. Users specify file names when uploading files holding user-generated documentation for JOC Cockpit. Specifically crafted file names allow an XSS attack to inject code that is executed with the browser. Risk of the vulnerability is considered high for branch 1.13 of JobScheduler (JS1). The vulnerability does not affect branch 2.x of JobScheduler (JS7) for releases after 2.1.0. The vulnerability is resolved with release 1.13.19.	6.3	More Details
CVE-2023-3581	Mattermost fails to properly validate the origin of a websocket connection allowing a MITM attacker on Mattermost to access the websocket APIs.	6.2	More Details
CVE-2023-37630	Online Piggery Management System 1.0 is vulnerable to Cross Site Scripting (XSS). An unauthenticated user can POST JavaScript code to "manage-breed.php" resulting in Persistent XSS.	6.1	More Details
CVE-2023-3708	Several themes for WordPress by DeoThemes are vulnerable to Reflected Cross-Site Scripting via breadcrumbs in various versions due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1893	The Login Configurator WordPress plugin through 2.1 does not properly escape a URL parameter before outputting it to the page, leading to a reflected cross-site scripting vulnerability targeting site administrators.	6.1	More Details
CVE-2023-2701	The Gravity Forms WordPress plugin before 2.7.5 does not escape generated URLs before outputting them in attributes, leading to Reflected Cross-Site Scripting which could be used against high-privileged users such as admin.	6.1	More Details
CVE-2023-30561	The data flowing between the PCU and its modules is insecure. A threat actor with physical access could potentially read or modify data by attaching a specially crafted device while an infusion is running.	6.1	More Details
CVE-2023-37947	Jenkins OpenShift Login Plugin 1.1.0.227.v27e08dfb_1a_20 and earlier improperly determines that a redirect URL after login is legitimately pointing to Jenkins, allowing attackers to perform phishing attacks.	6.1	More Details
CVE-2023-31852	Cudy LT400 1.13.4 is vulnerable to Cross Site Scripting (XSS) in cgi-bin/luci/admin/network/wireless/config via the iface parameter.	6.1	More Details
CVE-2023-2960	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Oliva Expertise Oliva Expertise EKS allows Cross-Site Scripting (XSS).This issue affects Oliva Expertise EKS: before 1.2.	6.1	More Details
CVE-2023-3041	The Autochat Automatic Conversation WordPress plugin through 1.1.7 does not sanitise and escape user input before outputting it back on the page, leading to a cross-site Scripting attack.	6.1	More Details
CVE-2023-3182	The Membership WordPress plugin before 3.2.3 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-31853	Cudy LT400 1.13.4 is vulnerable Cross Site Scripting (XSS) in /cgi-bin/luci/admin/network/bandwidth via the icon parameter.	6.1	More Details
CVE-2023-37746	A cross-site scripting (XSS) vulnerability in Maid Hiring Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Title parameter of the /admin/contactus.php component.	6.1	More Details
CVE-2023-31851	Cudy LT400 1.13.4 is has a cross-site scripting (XSS) vulnerability in /cgi-bin/luci/admin/network/wireless/status via the iface parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37743	A cross-site scripting (XSS) vulnerability in Teacher Subject Allocation System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Search text box.	6.1	More Details
CVE-2023-3672	Cross-site Scripting (XSS) - DOM in GitHub repository plaidweb/webmention.js prior to 0.5.5.	6.1	More Details
CVE-2023-33231	XSS attack was possible in DPA 2023.2 due to insufficient input validation	6.1	More Details
CVE-2023-37259	matrix-react-sdk is a react-based SDK for inserting a Matrix chat/voip client into a web page. The Export Chat feature includes certain attacker-controlled elements in the generated document without sufficient escaping, leading to stored Cross site scripting (XSS). Since the Export Chat feature generates a separate document, an attacker can only inject code run from the `null` origin, restricting the impact. However, the attacker can still potentially use the XSS to leak message contents. A malicious homeserver is a potential attacker since the affected inputs are controllable server-side. This issue has been addressed in commit `22fcd34c60` which is included in release version 3.76.0. Users are advised to upgrade. The only known workaround for this issue is to disable or to not use the Export Chat feature.	6.1	More Details
CVE-2023-37745	A cross-site scripting (XSS) vulnerability in Maid Hiring Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Page Description of the /admin/aboutus.php component.	6.1	More Details
CVE-2023-37744	Maid Hiring Management System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /admin/search-booking-request.php.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22055	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime SEC). Supported versions that are affected are Prior to 9.2.7.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2023-22035	Vulnerability in the Oracle Scripting product of Oracle E-Business Suite (component: iSurvey Module). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Scripting. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Scripting, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Scripting accessible data as well as unauthorized read access to a subset of Oracle Scripting accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2023-22042	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Diagnostics). Supported versions that are affected are 12.2.3-12.3.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data as well as unauthorized read access to a subset of Oracle Applications Framework accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37561	Open redirect vulnerability in ELECOM wireless LAN routers and ELECOM wireless LAN repeaters allows a remote unauthenticated attacker to redirect users to arbitrary web sites and conduct phishing attacks via a specially crafted URL. Affected products and versions are as follows: WRH-300WH-H v2.12 and earlier, WTC-300HWH v1.09 and earlier, WTC-C1167GC-B v1.17 and earlier, and WTC-C1167GC-W v1.17 and earlier.	6.1	More Details
CVE-2023-37560	Cross-site scripting vulnerability in WRH-300WH-H v2.12 and earlier, and WTC-300HWH v1.09 and earlier allows a remote unauthenticated attacker to inject an arbitrary script.	6.1	More Details
CVE-2023-21961	Vulnerability in the Oracle Hyperion Essbase Administration Services product of Oracle Essbase (component: EAS Administration and EAS Console). The supported version that is affected is 21.4.3.0.0. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Hyperion Essbase Administration Services executes to compromise Oracle Hyperion Essbase Administration Services. While the vulnerability is in Oracle Hyperion Essbase Administration Services, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Essbase Administration Services accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details
CVE-2023-37224	An issue in Archer Platform before v.6.13 fixed in v.6.12.0.6 and v.6.13.0 allows an authenticated attacker to obtain sensitive information via the log files.	6.0	More Details
CVE-2023-20210	A vulnerability in Cisco BroadWorks could allow an authenticated, local attacker to elevate privileges to the root user on an affected device. The vulnerability is due to insufficient input validation by the operating system CLI. An attacker could exploit this vulnerability by issuing a crafted command to the affected system. A successful exploit could allow the attacker to execute commands as the root user. To exploit this vulnerability, an attacker must have valid BroadWorks administrative privileges on the affected device.	6.0	More Details
CVE-2023-37468	Feedbacksystem is a personalized feedback system for students using artificial intelligence. Passwords of users using LDAP login are stored in clear text in the database. The LDAP users password is passed unencrypted in the LoginController.scala and stored in the database when logging in for the first time. Users using only local login or the cas login are not affected. This issue has been patched in version 1.19.2.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22053	Vulnerability in the MySQL Server product of Oracle MySQL (component: Client programs). Supported versions that are affected are 5.7.42 and prior and 8.0.33 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server and unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:H).	5.9	More Details
CVE-2023-22043	Vulnerability in Oracle Java SE (component: JavaFX). The supported version that is affected is Oracle Java SE: 8u371. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).	5.9	More Details
CVE-2023-29449	JavaScript preprocessing, webhooks and global scripts can cause uncontrolled CPU, memory, and disk I/O utilization. Preprocessing/webhook/global script configuration and testing are only available to Administrative roles (Admin and Superadmin). Administrative privileges should be typically granted to users who need to perform tasks that require more control over the system. The security risk is limited because not all users have this level of access.	5.9	More Details
CVE-2023-37943	Jenkins Active Directory Plugin 2.30 and earlier ignores the "Require TLS" and "StartTls" options and always performs the connection test to Active directory unencrypted, allowing attackers able to capture network traffic between the Jenkins controller and Active Directory servers to obtain Active Directory credentials.	5.9	More Details
CVE-2023-24390	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WeSecur Security plugin <= 1.2.1 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29458	Duktape is an 3rd-party embeddable JavaScript engine, with a focus on portability and compact footprint. When adding too many values in valstack JavaScript will crash. This issue occurs due to bug in Duktape 2.6 which is an 3rd-party solution that we use.	5.9	More Details
CVE-2022-47421	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Repute InfoSystems ARMember (free), Repute InfoSystems ARMember (premium) plugins.	5.9	More Details
CVE-2023-28021	The BigFix WebUI uses weak cipher suites.	5.9	More Details
CVE-2023-33329	Auth. (admin+) Reflected Cross-Site Scripting (XSS) vulnerability in Hijiri Custom Post Type Generator plugin <= 2.4.2 versions.	5.9	More Details
CVE-2023-3635	GzipSource does not handle an exception that might be raised when parsing a malformed gzip buffer. This may lead to denial of service of the Okio client when handling a crafted GZIP archive, by using the GzipSource class.	5.9	More Details
CVE-2023-36383	Auth. (editor+) Stored Cross-Site Scripting (XSS) vulnerability in MagePeople Team Event Manager and Tickets Selling Plugin for WooCommerce plugin <= 3.9.5 versions.	5.9	More Details
CVE-2021-31294	Redis before 6cbea7d allows a replica to cause an assertion failure in a primary server by sending a non-administrative command (specifically, a SET command). NOTE: this was fixed for Redis 6.2.x and 7.x in 2021. Versions before 6.2 were not intended to have safety guarantees related to this.	5.9	More Details
CVE-2023-2912	Use After Free vulnerability in Secomea SiteManager Embedded allows Obstruction.	5.9	More Details
CVE-2023-29456	URL validation scheme receives input from a user and then parses it to identify its various components. The validation scheme can ensure that all URL components comply with internet standards.	5.7	More Details
CVE-2023-3444	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.3 before 15.11.10, all versions starting from 16.0 before 16.0.6, all versions starting from 16.1 before 16.1.1, which allows an attacker to merge arbitrary code into protected branches.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37461	Metersphere is an opensource testing framework. Files uploaded to Metersphere may define a `belongType` value with a relative path like `../../../../` which may cause metersphere to attempt to overwrite an existing file in the defined location or to create a new file. Attackers would be limited to overwriting files that the metersphere process has access to. This issue has been addressed in version 2.10.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.6	More Details
CVE-2023-34143	Improper Validation of Certificate with Host Mismatch vulnerability in Hitachi Device Manager on Windows, Linux (Device Manager Server, Device Manager Agent, Host Data Collector components) allows Man in the Middle Attack.This issue affects Hitachi Device Manager: before 8.8.5-02.	5.6	More Details
CVE-2023-21983	Vulnerability in the Application Express Administration product of Oracle Application Express (component: None). Supported versions that are affected are Application Express Administration: 18.2-22.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Application Express Administration. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Application Express Administration accessible data as well as unauthorized read access to a subset of Application Express Administration accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Application Express Administration. CVSS 3.1 Base Score 5.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L).	5.6	More Details
CVE-2023-30930	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2020-36762	A vulnerability was found in ONS Digital RAS Collection Instrument up to 2.0.27 and classified as critical. Affected by this issue is the function jobs of the file .github/workflows/comment.yml. The manipulation of the argument $COMMENT_BODY leads to os command injection. Upgrading to version 2.0.28 is able to address this issue. The name of the patch is dcaad2540f7d50c512ff2e031d3778dd9337db2b. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-234248.	5.5	More Details
CVE-2023-30920	In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33888	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2020-23910	Stack-based buffer overflow vulnerability in asn1c through v0.9.28 via function genhash_get in genhash.c.	5.5	More Details
CVE-2020-23911	An issue was discovered in asn1c through v0.9.28. A NULL pointer dereference exists in the function _default_error_logger() located in asn1fix.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2023-30919	In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-33889	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2021-33294	In elfutils 0.183, an infinite loop was found in the function handle_symtab in readelf.c .Which allows attackers to cause a denial of service (infinite loop) via crafted file.	5.5	More Details
CVE-2023-33890	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-33891	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-33892	In fastDial service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-30918	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-30913	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-37200	A CWE-611: Improper Restriction of XML External Entity Reference vulnerability exists that could cause loss of confidentiality when replacing a project file on the local filesystem and after manual restart of the server.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31441	In NATO Communications and Information Agency anet (aka Advisor Network) through 3.3.0, an attacker can provide a crafted JSON file to sanitizeJson and cause an exception. This is related to the U+FFFD Unicode replacement character. A for loop does not consider that a data structure is being modified during loop execution.	5.5	More Details
CVE-2023-30931	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-28019	Insufficient validation in Bigfix WebUI API App site version < 14 allows an authenticated WebUI user to issue SQL queries via an unparameterized SQL query.	5.5	More Details
CVE-2023-33893	In fastDial service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-35763	Iagona ScrutisWeb versions 2.1.37 and prior are vulnerable to a cryptographic vulnerability that could allow an unauthenticated user to decrypt encrypted passwords into plaintext.	5.5	More Details
CVE-2023-33894	In fastDial service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-37139	ChakraCore branch master cbb9b was discovered to contain a stack overflow vulnerability via the function Js::ScopeSlots::IsDebuggerScopeSlotArray().	5.5	More Details
CVE-2023-33895	In fastDial service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-37140	ChakraCore branch master cbb9b was discovered to contain a segmentation violation via the function Js::DiagScopeVariablesWalker::GetChildrenCount().	5.5	More Details
CVE-2023-33898	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-33899	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37141	ChakraCore branch master cbb9b was discovered to contain a segmentation violation via the function Js::ProfilingHelpers::ProfiledNewScArray().	5.5	More Details
CVE-2023-37142	ChakraCore branch master cbb9b was discovered to contain a segmentation violation via the function Js::EntryPointInfo::HasInlinees().	5.5	More Details
CVE-2023-37143	ChakraCore branch master cbb9b was discovered to contain a segmentation violation via the function BackwardPass::IsEmptyLoopAfterMemOp().	5.5	More Details
CVE-2023-22017	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.46 and Prior to 7.0.10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: This vulnerability applies to Windows VMs only. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	5.5	More Details
CVE-2023-30921	In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2018-25088	A vulnerability, which was classified as critical, was found in Blue Yonder postgraas_server up to 2.0.0b2. Affected is the function _create_pg_connection/create_postgres_db of the file postgraas_server/backends/postgres_cluster/postgres_cluster_driver.py of the component PostgreSQL Backend Handler. The manipulation leads to sql injection. Upgrading to version 2.0.0 is able to address this issue. The patch is identified as 7cd8d016edc74a78af0d81c948bfafbcc93c937c. It is recommended to upgrade the affected component. VDB-234246 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2023-33887	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-30939	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30932	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-30933	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-30927	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-38409	An issue was discovered in set_con2fb_map in drivers/video/fbdev/core/fbcon.c in the Linux kernel before 6.2.12. Because an assignment occurs only for the first vc, the fbcon_registered_fb and fbcon_display arrays can be desynchronized in fbcon_mode_deleted (the con2fb_map points at the old fb_info).	5.5	More Details
CVE-2023-37476	OpenRefine is a free, open source tool for data processing. A carefully crafted malicious OpenRefine project tar file can be used to trigger arbitrary code execution in the context of the OpenRefine process if a user can be convinced to import it. The vulnerability exists in all versions of OpenRefine up to and including 3.7.3. Users should update to OpenRefine 3.7.4 as soon as possible. Users unable to upgrade should only import OpenRefine projects from trusted sources.	5.5	More Details
CVE-2023-30934	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-30935	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-30936	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-30937	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-37770	faust commit ee39a19 was discovered to contain a stack overflow via the component boxppShared::print() at /boxes/ppbox.cpp.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30938	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-30926	In opm service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-28864	Progress Chef Infra Server before 15.7 allows a local attacker to exploit a /var/opt/opscode/local-mode-cache/backup world-readable temporary backup path to access sensitive information, resulting in the disclosure of all indexed node data, because OpenSearch credentials are exposed. (The data typically includes credentials for additional systems.) The attacker must wait for an admin to run the "chef-server-ctl reconfigure" command.	5.5	More Details
CVE-2023-30940	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-30922	In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-30941	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-30942	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-30925	In opm service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-32788	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-32789	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33881	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-33882	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-33883	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-33884	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-30924	In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-33885	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-30923	In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-33886	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-33900	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-30226	An issue was discovered in function get_gnu_verneed in rizinorg Rizin prior to 0.5.0 verneed_entry allows attackers to cause a denial of service via crafted elf file.	5.5	More Details
CVE-2023-33901	In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29314	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-29317	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-29452	Currently, geomap configuration (Administration -> General -> Geographical maps) allows using HTML in the field “Attribution text” when selected “Other” Tile provider.	5.5	More Details
CVE-2023-29316	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-3433	The "nickname" field within Savoir-faire Linux's Jami application is susceptible to a failed state when a user inserts special characters into the field. When present, these special characters, make it so the application cannot create the signature for the user and results in a local denial of service to the application.	5.5	More Details
CVE-2023-29315	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-33902	In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-29313	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21260	In notification access permission dialog box, malicious application can embedded a very long service label that overflow the original user prompt and possibly contains mis-leading information to be appeared as a system message for user confirmation.	5.5	More Details
CVE-2023-29312	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-29311	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-29310	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-36838	An Out-of-bounds Read vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series allows a local, authenticated attacker with low privileges, to cause a Denial of Service (DoS). If a low privileged user executes a specific CLI command, flowd which is responsible for traffic forwarding in SRX crashes and generates a core dump. This will cause temporary traffic interruption until the flowd process is restarted automatically. Continued execution of this command will lead to a sustained DoS. This issue affects Juniper Networks Junos OS on SRX Series: All versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S4; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R3; 22.3 versions prior to 22.3R2; 22.4 versions prior to 22.4R1-S1, 22.4R2.	5.5	More Details
CVE-2023-29309	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2620	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.1 prior to 15.11.10, all versions from 16.0 prior to 16.0.6, all versions from 16.1 prior to 16.1.1. A maintainer could modify a webhook URL to leak masked webhook secrets by manipulating other masked portions. This addresses an incomplete fix for CVE-2023-0838.	5.5	More Details
CVE-2023-29318	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-21249	In multiple functions of OneTimePermissionUserManager.java, there is a possible one-time permission retention due to a permissions bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21239	In visitUris of Notification.java, there is a possible way to leak image data across user boundaries due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21240	In Policy of Policy.java, there is a possible boot loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-20942	In openMmapStream of AudioFlinger.cpp, there is a possible way to record audio without displaying the microphone privacy indicator due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2021-0948	The PVRSRVBridgeGetMultiCoreInfo ioctl in the PowerVR kernel driver can return uninitialized kernel memory to user space. The contents of this memory could contain sensitive information.	5.5	More Details
CVE-2023-38046	A vulnerability exists in Palo Alto Networks PAN-OS software that enables an authenticated administrator with the privilege to commit a specifically created configuration to read local files and resources from the system.	5.5	More Details
CVE-2023-21238	In visitUris of RemoteViews.java, there is a possible leak of images between users due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29319	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-36840	A Reachable Assertion vulnerability in Routing Protocol Daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows a locally-based, low-privileged attacker to cause a Denial of Service (DoS). On all Junos OS and Junos OS Evolved, when a specific L2VPN command is run, RPD will crash and restart. Continued execution of this specific command will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS All versions prior to 19.3R3-S10; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R2; Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S7-EVO; 21.1 versions prior to 21.1R3-S3-EVO; 21.2 versions prior to 21.2R3-S5-EVO; 21.3 versions prior to 21.3R3-S4-EVO; 21.4 versions prior to 21.4R3-EVO; 22.1 versions prior to 22.1R3-EVO; 22.2 versions prior to 22.2R2-EVO; 22.3 versions prior to 22.3R2-EVO;	5.5	More Details
CVE-2023-21243	In validateForCommonR1andR2 of PasspointConfiguration.java, there is a possible way to inflate the size of a config file with no limits due to a buffer overflow. This could lead to local denial of service with no additional execution privileges needed. User interaction is needed for exploitation.	5.5	More Details
CVE-2023-36266	An issue was discovered in Keeper Password Manager for Desktop version 16.10.2, and the KeeperFill Browser Extensions version 16.5.4, allows local attackers to gain sensitive information via plaintext password storage in memory after the user is already logged in, and may persist after logout. NOTE: the vendor disputes this for two reasons: the information is inherently available during a logged-in session when the attacker can read from arbitrary memory locations, and information only remains available after logout because of memory-management limitations of web browsers (not because the Keeper technology itself is retaining the information).	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22011	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). Supported versions that are affected are 6.4.0.0.0 and 7.0.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L).	5.4	More Details
CVE-2023-36656	Cross Site Scripting (XSS) vulnerability in Jaegertracing Jaeger UI before v.1.31.0 allows a remote attacker to execute arbitrary code via the KeyValuesTable component.	5.4	More Details
CVE-2023-29455	Reflected XSS attacks, also known as non-persistent attacks, occur when a malicious script is reflected off a web application to the victim's browser. The script is activated through a link, which sends a request to a website with a vulnerability that enables execution of malicious scripts.	5.4	More Details
CVE-2023-35880	Cross-Site Request Forgery (CSRF) vulnerability in WooCommerce WooCommerce Brands plugin <= 1.6.49 versions.	5.4	More Details
CVE-2023-36513	Cross-Site Request Forgery (CSRF) vulnerability in WooCommerce AutomateWoo plugin <= 5.7.5 versions.	5.4	More Details
CVE-2023-35096	Cross-Site Request Forgery (CSRF) vulnerability in myCred plugin <= 2.5 versions.	5.4	More Details
CVE-2023-37974	Cross-Site Request Forgery (CSRF) vulnerability in Justin Klein WP Social AutoConnect plugin <= 4.6.1 versions.	5.4	More Details
CVE-2023-37223	Cross Site Scripting (XSS) vulnerability in Archer Platform before v.6.13 and fixed in v.6.12.0.6 and v.6.13.0 allows a remote authenticated attacker to execute arbitrary code via a crafted malicious script.	5.4	More Details
CVE-2023-37968	Cross-Site Request Forgery (CSRF) vulnerability in Faboba Falang multilanguage for WordPress plugin <= 1.3.39 versions.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46857	Cross-Site Request Forgery (CSRF) vulnerability in SiteAlert plugin <= 1.9.7 versions.	5.4	More Details
CVE-2023-37455	The permission request prompt from the site in the background tab was overlaid on top of the site in the foreground tab. This vulnerability affects Firefox for iOS < 115.	5.4	More Details
CVE-2023-24896	Dynamics 365 Finance Spoofing Vulnerability	5.4	More Details
CVE-2023-35038	Cross-Site Request Forgery (CSRF) vulnerability in wpexperts.Io WP PDF Generator plugin <= 1.2.2 versions.	5.4	More Details
CVE-2023-3403	The ProfileGrid plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'pm_upload_csv' function in versions up to, and including, 5.5.1. This makes it possible for authenticated attackers, with subscriber-level permissions or above to import new users and update existing users.	5.4	More Details
CVE-2023-31705	A Reflected Cross-site scripting (XSS) vulnerability in Sourcecodester Task Reminder System 1.0 allows an authenticated user to inject malicious javascript into the page parameter.	5.4	More Details
CVE-2023-25473	Cross-Site Request Forgery (CSRF) vulnerability in Miro Mannino Flickr Justified Gallery plugin <= 3.5 versions.	5.4	More Details
CVE-2023-37963	A missing permission check in Jenkins Benchmark Evaluator Plugin 1.0.1 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL and to check for the existence of directories, `.csv`, and `.ycsb` files on the Jenkins controller file system.	5.4	More Details
CVE-2023-37386	Cross-Site Request Forgery (CSRF) vulnerability in Media Library Helper plugin <= 1.2.0 versions.	5.4	More Details
CVE-2023-37387	Cross-Site Request Forgery (CSRF) vulnerability in RadiusTheme Classified Listing plugin <= 2.4.5 versions.	5.4	More Details
CVE-2023-37973	Cross-Site Request Forgery (CSRF) vulnerability in David Pokorny Replace Word plugin <= 2.1 versions.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4417	The Forminator – Contact Form, Payment Form & Custom Form Builder plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.13.4. This is due to missing or incorrect nonce validation on the listen_for_saving_export_schedule() function. This makes it possible for unauthenticated attackers to export form submissions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	5.4	More Details
CVE-2023-2517	The Metform Elementor Contact Form Builder plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.3.2. This is due to missing or incorrect nonce validation on the permalink_setup function. This makes it possible for unauthenticated attackers to change the permalink structure via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. While nonce verification is implemented, verification only takes place when a nonce is provided.	5.4	More Details
CVE-2023-22020	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). Supported versions that are affected are 6.4.0.0.0 and 7.0.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	5.4	More Details
CVE-2023-2579	The InventoryPress WordPress plugin through 1.7 does not sanitise and escape some of its settings, which could allow users with the role of author and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22061	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Visual Analyzer). The supported version that is affected is 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2023-3319	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in iDisplay PlatPlay DS allows Stored XSS.This issue affects PlatPlay DS: before 3.14.	5.4	More Details
CVE-2023-22050	Vulnerability in the JD Edwards EnterpriseOne Orchestrator product of Oracle JD Edwards (component: E1 IOT Orchestrator Security). Supported versions that are affected are Prior to 9.2.7.4. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Orchestrator. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Orchestrator accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Orchestrator accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	5.4	More Details
CVE-2023-22039	Vulnerability in the Oracle Agile PLM product of Oracle Supply Chain (component: WebClient). The supported version that is affected is 9.3.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Agile PLM, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Agile PLM accessible data as well as unauthorized read access to a subset of Oracle Agile PLM accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38350	PNP4Nagios through 81ebfc5 has stored XSS in the AJAX controller via the basket API and filters. This affects 0.6.26.	5.4	More Details
CVE-2023-23719	Cross-Site Request Forgery (CSRF) vulnerability in Premmerce plugin <= 1.3.17 versions.	5.4	More Details
CVE-2023-27606	Cross-Site Request Forgery (CSRF) vulnerability in Sajjad Hossain WP Reroute Email plugin <= 1.4.6 versions.	5.4	More Details
CVE-2023-27424	Cross-Site Request Forgery (CSRF) vulnerability in Korol Yuriy aka Shra Inactive User Deleter plugin <= 1.59 versions.	5.4	More Details
CVE-2023-0439	The NEX-Forms WordPress plugin before 8.4.4 does not escape its form name, which could lead to Stored Cross-Site Scripting issues. By default only SuperAdmins (in multisite) / admins (in single site) can create forms, however there is a settings allowing them to give lower roles access to such feature.	5.4	More Details
CVE-2023-2143	The Enable SVG, WebP & ICO Upload WordPress plugin through 1.0.3 does not sanitize SVG file contents, leading to a Cross-Site Scripting vulnerability.	5.4	More Details
CVE-2023-29454	Stored or persistent cross-site scripting (XSS) is a type of XSS where the attacker first sends the payload to the web application, then the application saves the payload (e.g., in a database or server-side text files), and finally, the application unintentionally executes the payload for every victim visiting its web pages.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2975	Issue summary: The AES-SIV cipher implementation contains a bug that causes it to ignore empty associated data entries which are unauthenticated as a consequence. Impact summary: Applications that use the AES-SIV algorithm and want to authenticate empty data entries as associated data can be misled by removing, adding or reordering such empty entries as these are ignored by the OpenSSL implementation. We are currently unaware of any such applications. The AES-SIV algorithm allows for authentication of multiple associated data entries along with the encryption. To authenticate empty data the application has to call EVP_EncryptUpdate() (or EVP_CipherUpdate()) with NULL pointer as the output buffer and 0 as the input buffer length. The AES-SIV implementation in OpenSSL just returns success for such a call instead of performing the associated data authentication operation. The empty data thus will not be authenticated. As this issue does not affect non-empty associated data authentication and we expect it to be rare for an application to use empty associated data entries this is qualified as Low severity issue.	5.3	More Details
CVE-2023-3362	An information disclosure issue in GitLab CE/EE affecting all versions from 16.0 prior to 16.0.6, and version 16.1.0 allows unauthenticated actors to access the import error information if a project was imported from GitHub.	5.3	More Details
CVE-2023-34036	Reactive web applications that use Spring HATEOAS to produce hypermedia-based responses might be exposed to malicious forwarded headers if they are not behind a trusted proxy that ensures correctness of such headers, or if they don't have anything else in place to handle (and possibly discard) forwarded headers either in WebFlux or at the level of the underlying HTTP server. For the application to be affected, it needs to satisfy the following requirements: * It needs to use the reactive web stack (Spring WebFlux) and Spring HATEOAS to create links in hypermedia-based responses. * The application infrastructure does not guard against clients submitting (X-)Forwarded… headers.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37479	Open Enclave is a hardware-agnostic open source library for developing applications that utilize Hardware-based Trusted Execution Environments, also known as Enclaves. There are two issues that are mitigated in version 0.19.3. First, Open Enclave SDK does not properly sanitize the `MXCSR` register on enclave entry. This makes applications vulnerable to MXCSR Configuration Dependent Timing (MCDT) attacks, where incorrect `MXCSR` values can impact instruction retirement by at most one cycle, depending on the (secret) data operand value. Please find more details in the guidance from Intel in the references. Second, Open Enclave SDK does not sanitize x86's alignment check flag `RFLAGS.AC` on enclave entry. This opens up the possibility for a side-channel attacker to be notified for every unaligned memory access performed by the enclave. The issue has been addressed in version 0.19.3 and the current master branch. Users will need to recompile their applications against the patched libraries to be protected from this vulnerability. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2023-3649	iSCSI dissector crash in Wireshark 4.0.0 to 4.0.6 allows denial of service via packet injection or crafted capture file	5.3	More Details
CVE-2023-3648	Kafka dissector crash in Wireshark 4.0.0 to 4.0.6 and 3.6.0 to 3.6.14 allows denial of service via packet injection or crafted capture file	5.3	More Details
CVE-2023-33857	IBM InfoSphere Information Server 11.7 could allow a remote attacker to obtain system information using a specially crafted query that could aid in further attacks against the system. IBM X-Force ID: 257695.	5.3	More Details
CVE-2023-3709	The Royal Elementor Addons plugin for WordPress is vulnerable to unauthenticated API key disclosure in versions up to, and including, 1.3.70 due to the plugin adding the API key to the source code of any page running the MailChimp block. This makes it possible for unauthenticated attackers to obtain a site's MailChimp API key. We recommend resetting any MailChimp API keys if running a vulnerable version of this plugin with the MailChimp block enabled as the API key may have been compromised.	5.3	More Details
CVE-2023-34131	Exposure of sensitive information to an unauthorized actor vulnerability in SonicWall GMS and Analytics enables an unauthenticated attacker to access restricted web pages. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4023	The 3DPrint WordPress plugin before 3.5.6.9 does not protect against CSRF attacks in the modified version of Tiny File Manager included with the plugin, allowing an attacker to craft a malicious request that will create an archive of any files or directories on the target server by tricking a logged in admin into submitting a form. Furthermore the created archive has a predictable location and name, allowing the attacker to download the file if they know the time at which the form was submitted, making it possible to leak sensitive files like the WordPress configuration containing database credentials and secrets.	5.3	More Details
CVE-2023-30559	The firmware update package for the wireless card is not properly signed and can be modified.	5.2	More Details
CVE-2023-22041	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK executes to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	5.1	More Details
CVE-2023-22054	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22056	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2023-22057	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2023-20207	A vulnerability in the logging component of Cisco Duo Authentication Proxy could allow an authenticated, remote attacker to view sensitive information in clear text on an affected system. This vulnerability exists because certain unencrypted credentials are stored. An attacker could exploit this vulnerability by accessing the logs on an affected system and obtaining credentials that they may not normally have access to. A successful exploit could allow the attacker to view sensitive information in clear text.	4.9	More Details
CVE-2023-22046	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2023-21950	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22007	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.41 and prior and 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2023-22008	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2023-28023	A cross site request forgery vulnerability in the BigFix WebUI Software Distribution interface site version 44 and before allows an NMO attacker to access files on server side systems (server machine and all the ones in its network).	4.9	More Details
CVE-2023-22034	Vulnerability in the Unified Audit component of Oracle Database Server. Supported versions that are affected are 19.3-19.19 and 21.3-21.10. Easily exploitable vulnerability allows high privileged attacker having SYSDBA privilege with network access via Oracle Net to compromise Unified Audit. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Unified Audit accessible data. CVSS 3.1 Base Score 4.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N).	4.9	More Details
CVE-2023-37785	A cross-site scripting (XSS) vulnerability in ImpressCMS v1.4.5 and before allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the smile_code parameter of the component /editprofile.php.	4.8	More Details
CVE-2023-37786	Multiple cross-site scripting (XSS) vulnerabilities in Geeklog v2.2.2 allow attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Mail Settings[backend], Mail Settings[host], Mail Settings[port] and Mail Settings[auth] parameters of the /admin/configuration.php.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3245	The Floating Chat Widget WordPress plugin before 3.1.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2023-37787	Multiple cross-site scripting (XSS) vulnerabilities in Geeklog v2.2.2 allow attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Rule and Route parameters of /admin/router.php.	4.8	More Details
CVE-2023-3591	Mattermost fails to invalidate previously generated password reset tokens when a new reset token was created.	4.8	More Details
CVE-2023-0160	A deadlock flaw was found in the Linux kernel's BPF subsystem. This flaw allows a local user to potentially crash the system.	4.7	More Details
CVE-2023-36836	A Use of an Uninitialized Resource vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a local, authenticated attacker with low privileges to cause a Denial of Service (DoS). On all Junos OS and Junos OS Evolved platforms, in a Multicast only Fast Reroute (MoFRR) scenario, the rpd process can crash when a a specific low privileged CLI command is executed. The rpd crash will impact all routing protocols until the process has automatically been restarted. As the operational state which makes this issue exploitable is outside the attackers control, this issue is considered difficult to exploit. Continued execution of this command will lead to a sustained DoS. This issue affects: Juniper Networks Junos OS 19.4 version 19.4R3-S5 and later versions prior to 19.4R3-S9; 20.1 version 20.1R2 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R3-S1; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R1-S2, 22.1R2; 22.2 versions prior to 22.2R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S6-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-S1-EVO; 21.4-EVO versions prior to 21.4R3-EVO; 22.1-EVO versions prior to 22.1R1-S2-EVO, 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO.	4.7	More Details
CVE-2023-29451	Specially crafted string can cause a buffer overrun in the JSON parser library leading to a crash of the Zabbix Server or a Zabbix Proxy.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38253	An out-of-bounds read flaw was found in w3m, in the growbuf_to_Str function in indep.c. This issue may allow an attacker to cause a denial of service through a crafted HTML file.	4.7	More Details
CVE-2023-38252	An out-of-bounds read flaw was found in w3m, in the Strnew_size function in Str.c. This issue may allow an attacker to cause a denial of service through a crafted HTML file.	4.7	More Details
CVE-2023-28020	URL redirection in Login page in HCL BigFix WebUI allows malicious user to redirect the client browser to an external site via redirect URL response header.	4.7	More Details
CVE-2023-38066	In JetBrains TeamCity before 2023.05.1 reflected XSS via the Referer header was possible during artifact downloads	4.6	More Details
CVE-2023-38063	In JetBrains TeamCity before 2023.05.1 stored XSS while running custom builds was possible	4.6	More Details
CVE-2023-38065	In JetBrains TeamCity before 2023.05.1 stored XSS while viewing the build log was possible	4.6	More Details
CVE-2023-38061	In JetBrains TeamCity before 2023.05.1 stored XSS when using a custom theme was possible	4.6	More Details
CVE-2023-37598	A Cross Site Request Forgery (CSRF) vulnerability in issabel-pbx v.4.0.0-6 allows a remote attacker to cause a denial of service via the delete new virtual fax function.	4.5	More Details
CVE-2023-33905	In iwnpi server, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	4.4	More Details
CVE-2023-22058	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.33 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33904	In hci_server, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	4.4	More Details
CVE-2023-33897	In libimpl-ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	4.4	More Details
CVE-2023-33896	In libimpl-ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	4.4	More Details
CVE-2023-22033	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.33 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details
CVE-2023-22005	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.33 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details
CVE-2023-22031	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 14.1.1.0.0 and 12.2.1.4.0. Difficult to exploit vulnerability allows high privileged attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3369	The About Me 3000 widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in versions up to, and including, 2.2.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2023-33903	In FM service, there is a possible missing params check. This could lead to local denial of service with System execution privileges needed.	4.4	More Details
CVE-2023-3434	Improper Input Validation in the hyperlink interpretation in Savoir-faire Linux's Jami (version 20222284) on Windows. This allows an attacker to send a custom HTML anchor tag to pass a string value to the Windows QRC Handler through the Jami messenger.	4.4	More Details
CVE-2022-48450	In bluetooth service, there is a possible missing params check. This could lead to local denial of service with System execution privileges needed.	4.4	More Details
CVE-2021-4410	The Qtranslate Slug plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.18. This is due to missing or incorrect nonce validation on the save_postdata() function. This makes it possible for unauthenticated attackers to save post data via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4408	The DW Question & Answer plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.5.8. This is due to missing or incorrect nonce validation on the update_answer() function. This makes it possible for unauthenticated attackers to update answers to questions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4424	The Slider Hero plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 8.2.0. This is due to missing or incorrect nonce validation on the qc_slider_hero_duplicate() function. This makes it possible for unauthenticated attackers to duplicate slides via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4426	The Absolute Reviews plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.0.8. This is due to missing or incorrect nonce validation on the metabox_review_save() function. This makes it possible for unauthenticated attackers to save meta tags via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4407	The Custom Banners plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.2.2 This is due to missing or incorrect nonce validation on the saveCustomFields() function. This makes it possible for unauthenticated attackers to save custom fields via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4425	The Defender Security plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.4.6. This is due to missing or incorrect nonce validation on the verify_otp_login_time() function. This makes it possible for unauthenticated attackers to verify a one time login via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4423	The RAYS Grid plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2.2. This is due to missing or incorrect nonce validation on the rsgd_insert_update() function. This makes it possible for unauthenticated attackers to update post fields via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2020-36761	The Top 10 plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.10.4. This is due to missing or incorrect nonce validation on the tptn_export_tables() function. This makes it possible for unauthenticated attackers to generate an export of the top 10 table via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2020-36760	The Ocean Extra plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.6.5]. This is due to missing or incorrect nonce validation on the add_core_extensions_bundle_validation() function. This makes it possible for unauthenticated attackers to validate extension bundles via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4409	The WooCommerce Etsy Integration plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.3.1. This is due to missing or incorrect nonce validation on the etcpf_delete_feed() function. This makes it possible for unauthenticated attackers to delete an export feed via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4411	The WP EasyPay – Square for WordPress plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.2.0. This is due to missing or incorrect nonce validation on the wpep_download_transaction_in_excel() function. This makes it possible for unauthenticated attackers to trigger a transactions download via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4416	The wp-mpdf plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.5.1. This is due to missing or incorrect nonce validation on the mpdf_admin_savepost() function. This makes it possible for unauthenticated attackers to save post data via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-3202	The MStore API plugin for WordPress is vulnerable to Cross-Site Request Forgery due to missing nonce validation on the mstore_update_firebase_server_key function. This makes it possible for unauthenticated attackers to update the firebase server key to push notification when order status changed via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4419	The WP-Backgrounds Lite plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.3. This is due to missing or incorrect nonce validation on the ino_save_data() function. This makes it possible for unauthenticated attackers to save meta data via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4422	The POST SMTP Mailer plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.0.20. This is due to missing or incorrect nonce validation on the handleCsvExport() function. This makes it possible for unauthenticated attackers to trigger a CSV export via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4421	The Advanced Popups plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.1. This is due to missing or incorrect nonce validation on the metabox_popup_save() function. This makes it possible for unauthenticated attackers to save meta tags via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-22012	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). The supported version that is affected is 7.0.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	4.3	More Details
CVE-2023-3199	The MStore API plugin for WordPress is vulnerable to Cross-Site Request Forgery due to missing nonce validation on the mstore_update_status_order_title function. This makes it possible for unauthenticated attackers to update status order title via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-22013	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). Supported versions that are affected are 6.4.0.0.0 and 7.0.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	4.3	More Details
CVE-2020-36752	The Coming Soon & Maintenance Mode Page plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.57. This is due to missing or incorrect nonce validation on the save_meta_box() function. This makes it possible for unauthenticated attackers to save meta boxes via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22021	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). Supported versions that are affected are 6.4.0.0.0 and 7.0.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	4.3	More Details
CVE-2023-2869	The WP-Members Membership plugin for WordPress is vulnerable to unauthorized plugin settings update due to a missing capability check on the do_field_reorder function in versions up to, and including, 3.4.7.3. This makes it possible for authenticated attackers with subscriber-level access to reorder form elements on login forms.	4.3	More Details
CVE-2021-4414	The Abandoned Cart Lite for WooCommerce plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 5.8.5. This is due to missing or incorrect nonce validation on the wcal_preview_emails() function. This makes it possible for unauthenticated attackers to generate email preview templates via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2020-36756	The 10WebAnalytics plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2.8. This is due to missing or incorrect nonce validation on the create_csv_file() function. This makes it possible for unauthenticated attackers to create a CSV file via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4413	The Process Steps Template Designer plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2.1. This is due to missing or incorrect nonce validation on the save() function. This makes it possible for unauthenticated attackers to save field icons via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-2562	The Gallery Metabox for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the refresh_metabox function in versions up to, and including, 1.5. This makes it possible for subscriber-level attackers to obtain a list of images attached to a post.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36757	The WP Hotel Booking plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.10.1. This is due to missing or incorrect nonce validation on the admin_add_order_item() function. This makes it possible for unauthenticated attackers to add an order item via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-2561	The Gallery Metabox for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the gallery_remove function in versions up to, and including, 1.5. This makes it possible for subscriber-level attackers to modify galleries attached to posts and pages with this plugin.	4.3	More Details
CVE-2023-22027	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). The supported version that is affected is 7.0.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	4.3	More Details
CVE-2023-2576	An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.7 before 15.11.10, all versions starting from 16.0 before 16.0.6, all versions starting from 16.1 before 16.1.1. This allowed a developer to remove the CODEOWNERS rules and merge to a protected branch.	4.3	More Details
CVE-2021-4412	The WP Prayer plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.6.5. This is due to missing or incorrect nonce validation on the save() and export() functions. This makes it possible for unauthenticated attackers to save plugin settings and trigger a data export via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4427	The Vuukle Comments, Reactions, Share Bar, Revenue plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.4.31. This is due to missing or incorrect nonce validation in the /admin/partials/free-comments-for-wordpress-vuukle-admin-display.php file. This makes it possible for unauthenticated attackers to edit the plugins settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4415	The Sunshine Photo Cart plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.8.28 This is due to missing or incorrect nonce validation on the sunshine_products_quicksave_post() function. This makes it possible for unauthenticated attackers to save custom post data via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4420	The Sell Media plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.5.5. This is due to missing or incorrect nonce validation on the sell_media_process() function. This makes it possible for unauthenticated attackers to sell media paypal orders via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-22004	Vulnerability in the Oracle Applications Technology product of Oracle E-Business Suite (component: Reports Configuration). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Technology accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).	4.3	More Details
CVE-2023-22009	Vulnerability in the Oracle Self-Service Human Resources product of Oracle E-Business Suite (component: Workforce Management). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Self-Service Human Resources. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Self-Service Human Resources accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	4.3	More Details
CVE-2022-47172	Cross-Site Request Forgery (CSRF) vulnerability in HasThemes ShopLentor plugin <= 2.6.2 versions.	4.3	More Details
CVE-2022-38062	Cross-Site Request Forgery (CSRF) vulnerability in Metagauss Download Theme plugin <= 1.0.9 versions.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45828	Cross-Site Request Forgery (CSRF) vulnerability in NooTheme Noo Timetable plugin <= 2.1.3 versions.	4.3	More Details
CVE-2023-38067	In JetBrains TeamCity before 2023.05.1 build parameters of the "password" type could be written to the agent log	4.3	More Details
CVE-2023-3585	Mattermost Boards fail to properly validate a board link, allowing an attacker to crash a channel by posting a specially crafted boards link.	4.3	More Details
CVE-2023-3582	Mattermost fails to verify channel membership when linking a board to a channel allowing a low-privileged authenticated user to link a Board to a private channel they don't have access to,	4.3	More Details
CVE-2023-36883	Microsoft Edge for iOS Spoofing Vulnerability	4.3	More Details
CVE-2023-37985	Cross-Site Request Forgery (CSRF) vulnerability in FiveStarPlugins Restaurant Menu and Food Ordering plugin <= 2.4.6 versions.	4.3	More Details
CVE-2023-3642	A vulnerability was found in GZ Scripts Vacation Rental Website 1.8 and classified as problematic. Affected by this issue is some unknown functionality of the file /VacationRentalWebsite/property/8/ad-has-principes/ of the component HTTP POST Request Handler. The manipulation of the argument username/title/comment leads to cross site scripting. The attack may be launched remotely. The identifier of this vulnerability is VDB-233888.	4.3	More Details
CVE-2022-36424	Cross-Site Request Forgery (CSRF) vulnerability in Nikola Loncar Easy Appointments plugin <= 3.11.9 versions.	4.3	More Details
CVE-2020-36750	The EWWW Image Optimizer plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 5.8.1. This is due to missing or incorrect nonce validation on the ewww_ngg_bulk_init() function. This makes it possible for unauthenticated attackers to perform bulk image optimization via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37945	A missing permission check in Jenkins SAML Single Sign On(SSO) Plugin 2.1.0 through 2.3.0 (both inclusive) allows attackers with Overall/Read permission to download a string representation of the current security realm.	4.3	More Details
CVE-2023-36511	Cross-Site Request Forgery (CSRF) vulnerability in WooCommerce WooCommerce Order Barcodes plugin <= 1.6.4 versions.	4.3	More Details
CVE-2023-38064	In JetBrains TeamCity before 2023.05.1 build chain parameters of the "password" type could be written to the agent log	4.3	More Details
CVE-2023-3614	Mattermost fails to properly validate a gif image file, allowing an attacker to consume a significant amount of server resources, making the server unresponsive for an extended period of time by linking to specially crafted image file.	4.3	More Details
CVE-2023-37950	A missing permission check in Jenkins mabl Plugin 0.0.46 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details
CVE-2023-38062	In JetBrains TeamCity before 2023.05.1 parameters of the "password" type could be shown in the UI in certain composite build configurations	4.3	More Details
CVE-2023-35089	Cross-Site Request Forgery (CSRF) vulnerability in Really Simple Plugins Recipe Maker For Your Food Blog from Zip Recipes plugin <= 8.0.7 versions.	4.3	More Details
CVE-2023-3641	A vulnerability has been found in khodakhah NodCMS 3.4.1 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /en/blog-comment-4 of the component POST Request Handler. The manipulation of the argument comment_name/comment_content leads to cross site scripting. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-233887.	4.3	More Details
CVE-2023-22672	Cross-Site Request Forgery (CSRF) vulnerability in Mr.Vibe vSlider Multi Image Slider for WordPress plugin <= 4.1.2 versions.	4.3	More Details
CVE-2023-23646	Cross-Site Request Forgery (CSRF) vulnerability in A WP Life Album Gallery – WordPress Gallery plugin <= 1.4.9 versions.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37892	Cross-Site Request Forgery (CSRF) vulnerability in Kemal YAZICI - PluginPress Shortcode IMDB plugin <= 6.0.8 versions.	4.3	More Details
CVE-2023-37889	Cross-Site Request Forgery (CSRF) vulnerability in WPAdmin WPAdmin AWS CDN plugin <= 2.0.13 versions.	4.3	More Details
CVE-2023-25036	Cross-Site Request Forgery (CSRF) vulnerability in akhlesh-nagar, a.Ankit Social Media Icons Widget plugin <= 1.6 versions.	4.3	More Details
CVE-2023-31216	Cross-Site Request Forgery (CSRF) vulnerability in Ultimate Member plugin <= 2.6.0 versions.	4.3	More Details
CVE-2022-47169	Cross-Site Request Forgery (CSRF) vulnerability in StaxWP Visibility Logic for Elementor plugin <= 2.3.4 versions.	4.3	More Details
CVE-2023-37954	A cross-site request forgery (CSRF) vulnerability in Jenkins Rebuilder Plugin 320.v5a_0933a_e7d61 and earlier allows attackers to rebuild a previous build.	4.3	More Details
CVE-2023-25482	Cross-Site Request Forgery (CSRF) vulnerability in Mike Martel WP Tiles plugin <= 1.1.2 versions.	4.3	More Details
CVE-2023-25475	Cross-Site Request Forgery (CSRF) vulnerability in Vladimir Prelovac Smart YouTube PRO plugin <= 4.3 versions.	4.3	More Details
CVE-2023-3593	Mattermost fails to properly validate markdown, allowing an attacker to crash the server via a specially crafted markdown input.	4.3	More Details
CVE-2023-3586	Mattermost fails to disable public Boards after the "Enable Publicly-Shared Boards" configuration option is disabled, resulting in previously-shared public Boards to remain accessible.	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22016	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.46 and Prior to 7.0.10. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 4.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:H).	4.2	More Details
CVE-2023-2200	An issue has been discovered in GitLab CE/EE affecting all versions starting from 7.14 before 15.11.10, all versions starting from 16.0 before 16.0.6, all versions starting from 16.1 before 16.1.1, which allows an attacker to inject HTML in an email address field.	4.1	More Details
CVE-2022-48451	In bluetooth service, there is a possible out of bounds write due to race condition. This could lead to local denial of service with System execution privileges needed.	4.1	More Details
CVE-2023-3363	An information disclosure issue in Gitlab CE/EE affecting all versions from 13.6 prior to 15.11.10, all versions from 16.0 prior to 16.0.6, all versions from 16.1 prior to 16.1.1, resulted in the Sidekiq log including webhook tokens when the log format was set to `default`.	3.9	More Details
CVE-2023-21949	Vulnerability in the Advanced Networking Option component of Oracle Database Server. Supported versions that are affected are 19.3-19.19 and 21.3-21.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Advanced Networking Option. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Advanced Networking Option accessible data. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22045	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	3.7	More Details
CVE-2023-22036	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Utility). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22049	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	3.7	More Details
CVE-2023-22051	Vulnerability in the Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: GraalVM Compiler). Supported versions that are affected are Oracle GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	3.7	More Details
CVE-2023-37948	Jenkins Oracle Cloud Infrastructure Compute Plugin 1.0.16 and earlier does not validate SSH host keys when connecting OCI clouds, enabling man-in-the-middle attacks.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22044	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	3.7	More Details
CVE-2023-3659	A vulnerability has been found in SourceCodester AC Repair and Services System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file admin/?page=user/manage_user. The manipulation of the argument firstname/middlename leads to cross site scripting. The attack can be launched remotely. The identifier VDB-234013 was assigned to this vulnerability.	3.5	More Details
CVE-2023-3684	A vulnerability was found in LivelyWorks Articart 2.0.1 and classified as problematic. Affected by this issue is some unknown functionality of the file /change-language/de_DE of the component Base64 Encoding Handler. The manipulation of the argument redirectTo leads to open redirect. The attack may be launched remotely. VDB-234230 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2022-4952	A vulnerability has been found in OmniSharp csharp-language-server-protocol up to 0.19.6 and classified as problematic. This vulnerability affects the function CreateSerializerSettings of the file src/JsonRpc/Serialization/SerializerBase.cs of the component JSON Serializer. The manipulation leads to resource consumption. Upgrading to version 0.19.7 is able to address this issue. The patch is identified as 7fd2219f194a9ef2a8901bb131c5fa12272305ce. It is recommended to upgrade the affected component. VDB-234238 is the identifier assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3681	A vulnerability classified as problematic was found in Campcodes Retro Cellphone Online Store 1.0. This vulnerability affects unknown code of the file /admin/modal_add_product.php. The manipulation of the argument description leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-234226 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-30565	An insecure connection between Systems Manager and CQI Reporter application could expose infusion data to an attacker.	3.5	More Details
CVE-2023-3691	A vulnerability, which was classified as problematic, was found in layui up to v2.8.0-rc.16. This affects an unknown part of the component HTML Attribute Handler. The manipulation of the argument title leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 2.8.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-234237 was assigned to this vulnerability.	3.5	More Details
CVE-2023-36466	Discourse is an open source discussion platform. When editing a topic, there is a vulnerability that enables a user to bypass the topic title validations for things like title length, number of emojis in title and blank topic titles. The issue is patched in the latest stable, beta and tests-passed version of Discourse.	3.5	More Details
CVE-2023-3685	A vulnerability was found in Nesote Inout Search Engine AI Edition 1.1. It has been classified as problematic. This affects an unknown part of the file /index.php. The manipulation of the argument page leads to cross site scripting. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-234231. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3613	Mattermost WelcomeBot plugin fails to to validate the membership status when inviting or adding users to channels allowing guest accounts to be added or invited to channels by default.	3.5	More Details
CVE-2023-3577	Mattermost fails to properly restrict requests to localhost/intranet during the interactive dialog, which could allow an attacker to perform a limited blind SSRF.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3683	A vulnerability has been found in LivelyWorks Articart 2.0.1 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /items/search. The manipulation of the argument search_term leads to cross site scripting. The attack can be launched remotely. The identifier VDB-234229 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2021-43760	Adobe Media Encoder versions 22.0, 15.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious MOV file.	3.3	More Details
CVE-2021-43759	Adobe Media Encoder versions 22.0, 15.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious MP4 file.	3.3	More Details
CVE-2023-33880	In music service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	3.3	More Details
CVE-2023-33879	In music service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	3.3	More Details
CVE-2023-38069	In JetBrains IntelliJ IDEA before 2023.1.4 license dialog could be suppressed in certain cases	3.3	More Details
CVE-2023-21246	In ShortcutInfo of ShortcutInfo.java, there is a possible way for an app to retain notification listening access due to an uncaught exception. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details
CVE-2021-44696	Adobe Prelude version 22.1.1 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious JPEG file.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43758	Adobe Media Encoder versions 22.0, 15.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious MP4 file.	3.3	More Details
CVE-2023-3590	Mattermost fails to delete card attachments in Boards, allowing an attacker to access deleted attachments.	3.1	More Details
CVE-2023-3584	Mattermost fails to properly check the authorization of POST /api/v4/teams when passing a team override scheme ID in the request, allowing an authenticated attacker with knowledge of a Team Override Scheme ID to create a new team with said team override scheme.	3.1	More Details
CVE-2023-22006	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37275	Auto-GPT is an experimental open-source application showcasing the capabilities of the GPT-4 language model. The Auto-GPT command line UI makes heavy use of color-coded print statements to signify different types of system messages to the user, including messages that are crucial for the user to review and control which commands should be executed. Before v0.4.3, it was possible for a malicious external resource (such as a website browsed by Auto-GPT) to cause misleading messages to be printed to the console by getting the LLM to regurgitate JSON encoded ANSI escape sequences (`\u001b[`). These escape sequences were JSON decoded and printed to the console as part of the model's "thinking process". The issue has been patched in release version 0.4.3.	3.1	More Details
CVE-2023-22048	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Pluggable Auth). Supported versions that are affected are 8.0.33 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N).	3.1	More Details
CVE-2023-21262	In startInput of AudioPolicyInterfaceImpl.cpp, there is a possible way of erroneously displaying the microphone privacy indicator due to a race condition. This could lead to false user expectations. User interaction is needed for exploitation.	3.1	More Details
CVE-2023-22052	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19.3-19.19 and 21.3-21.10. Difficult to exploit vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via multiple protocols to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java VM accessible data. CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N).	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37481	Fides is an open-source privacy engineering platform for managing data privacy requests and privacy regulations. The Fides webserver is vulnerable to a type of Denial of Service (DoS) attack. Attackers can exploit this vulnerability to upload zip files containing malicious SVG bombs (similar to a billion laughs attack), causing resource exhaustion in Admin UI browser tabs and creating a persistent denial of service of the 'new connector' page (`datastore-connection/new`). This vulnerability affects Fides versions `2.11.0` through `2.15.1`. Exploitation is limited to users with elevated privileges with the `CONNECTOR_TEMPLATE_REGISTER` scope, which includes root users and users with the owner role. The vulnerability has been patched in Fides version `2.16.0`. Users are advised to upgrade to this version or later to secure their systems against this threat. There is no known workaround to remediate this vulnerability without upgrading.	2.7	More Details
CVE-2023-37480	Fides is an open-source privacy engineering platform for managing data privacy requests and privacy regulations. The Fides webserver is vulnerable to a type of Denial of Service (DoS) attack. Attackers can exploit a weakness in the connector template upload feature to upload a malicious zip bomb file, resulting in resource exhaustion and service unavailability for all users of the Fides webserver. This vulnerability affects Fides versions `2.11.0` through `2.15.1`. Exploitation is limited to users with elevated privileges with the `CONNECTOR_TEMPLATE_REGISTER` scope, which includes root users and users with the owner role. The vulnerability has been patched in Fides version `2.16.0`. Users are advised to upgrade to this version or later to secure their systems against this threat. There is no known workaround to remediate this vulnerability without upgrading. If an attack occurs, the impact can be mitigated by manually or automatically restarting the affected container.	2.7	More Details
CVE-2023-3587	Mattermost fails to properly show information in the UI, allowing a system admin to modify a board state allowing any user with a valid sharing link to join the board with editor access, without the UI showing the updated permissions.	2.7	More Details
CVE-2023-22038	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).	2.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35901	IBM Robotic Process Automation 21.0.0 through 21.0.7.6 and 23.0.0 through 23.0.6 is vulnerable to client side validation bypass which could allow invalid changes or values in some fields. IBM X-Force ID: 259380.	2.7	More Details
CVE-2021-4428	A vulnerability has been found in what3words Autosuggest Plugin up to 4.0.0 on WordPress and classified as problematic. Affected by this vulnerability is the function enqueue_scripts of the file w3w-autosuggest/public/class-w3w-autosuggest-public.php of the component Setting Handler. The manipulation leads to information disclosure. The attack can be launched remotely. Upgrading to version 4.0.1 is able to address this issue. The patch is named dd59cbac5f86057d6a73b87007c08b8bfa0c32ac. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-234247.	2.7	More Details
CVE-2023-3660	A vulnerability was found in Campcodes Retro Cellphone Online Store 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/add_user_modal.php. The manipulation of the argument un leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-234014 is the identifier assigned to this vulnerability.	2.4	More Details
CVE-2023-22010	Vulnerability in Oracle Essbase (component: Security and Provisioning). The supported version that is affected is 21.4.3.0.0. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Essbase. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Essbase accessible data. CVSS 3.1 Base Score 2.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N).	2.2	More Details
CVE-2023-31007	Improper Authentication vulnerability in Apache Software Foundation Apache Pulsar Broker allows a client to stay connected to a broker after authentication data expires if the client connected through the Pulsar Proxy when the broker is configured with authenticateOriginalAuthData=false or if a client connects directly to a broker with a specially crafted connect command when the broker is configured with authenticateOriginalAuthData=false. This issue affects Apache Pulsar: through 2.9.4, from 2.10.0 through 2.10.3, 2.11.0. 2.9 Pulsar Broker users should upgrade to at least 2.9.5. 2.10 Pulsar Broker users should upgrade to at least 2.10.4. 2.11 Pulsar Broker users should upgrade to at least 2.11.1. 3.0 Pulsar Broker users are unaffected. Any users running the Pulsar Broker for 2.8.* and earlier should upgrade to one of the above patched versions.	0.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36168	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-37803	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-37809	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-37810	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-37811	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-37806	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-37805	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-21261	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-36119	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-37850	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-37804	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37802	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-36166	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-37801	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-3496	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-3418	Rejected reason: The issue is not in the plugin itself but the underlying chat service	N/A	More Details
CVE-2023-37800	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-37808	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-36120	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-36169	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-38326	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-36165	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-37807	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details