SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 19 April 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-2023-30537	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with the right to add an object on a page can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the styles properties `FlamingoThemesCode.WebHome`. This page is installed by default. The vulnerability has been patched in XWiki versions 13.10.11, 14.4.7 and 14.10.	9.9	More Details
CVE-2023-29209	XWiki Commons are technical libraries common to several other top level XWiki projects. Any user with view rights on commonly accessible documents including the legacy notification activity macro can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the macro parameters of the legacy notification activity macro. This macro is installed by default in XWiki. The vulnerability can be exploited via every wiki page that is editable including the user's profile, but also with just view rights using the HTMLConverter that is part of the CKEditor integration which is bundled with XWiki. The vulnerability has been patched in XWiki 13.10.11, 14.4.7 and 14.10.	9.9	More Details
CVE-2023-29214	XWiki Commons are technical libraries common to several other top level XWiki projects. Any user with edit rights can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the included pages in the IncludedDocuments panel. The problem has been patched on XWiki 14.4.7, and 14.10.	9.9	More Details
CVE-2023-29212	XWiki Commons are technical libraries common to several other top level XWiki projects. Any user with edit rights can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the included pages in the included documents edit panel. The problem has been patched on XWiki 14.4.7, and 14.10.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29211	XWiki Commons are technical libraries common to several other top level XWiki projects. Any user with view rights `WikiManager.DeleteWiki` can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the `wikiId` url parameter. The problem has been patched on XWiki 13.10.11, 14.4.7, and 14.10.	9.9	More Details
CVE-2023-29511	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with edit rights on a page (e.g., it's own user page), can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the section ids in `XWiki.AdminFieldsDisplaySheet`. This page is installed by default. The vulnerability has been patched in XWiki versions 15.0-rc-1, 14.10.1, 14.4.8, and 13.10.11.	9.9	More Details
CVE-2023-29210	XWiki Commons are technical libraries common to several other top level XWiki projects. Any user with view rights on commonly accessible documents including the notification preferences macros can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the user parameter of the macro that provide the notification filters. These macros are used in the user profiles and thus installed by default in XWiki. The vulnerability has been patched in XWiki 13.10.11, 14.4.7 and 14.10.	9.9	More Details
CVE-2023-29205	XWiki Commons are technical libraries common to several other top level XWiki projects. The HTML macro does not systematically perform a proper neutralization of script-related html tags. As a result, any user able to use the html macro in XWiki, is able to introduce an XSS attack. This can be particularly dangerous since in a standard wiki, any user is able to use the html macro directly in their own user profile page. The problem has been patched in XWiki 14.8RC1. The patch involves the HTML macros and are systematically cleaned up whenever the user does not have the script correct.	9.9	More Details
CVE-2023-29509	XWiki Commons are technical libraries common to several other top level XWiki projects. Any user with view rights on commonly accessible documents can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the `documentTree` macro parameters in This macro is installed by default in `FlamingoThemesCode.WebHome`. This page is installed by default. The vulnerability has been patched in XWiki 13.10.11, 14.4.7 and 14.10.	9.9	More Details
CVE-2023-2106	Weak Password Requirements in GitHub repository janeczku/calibre-web prior to 0.6.20.	9.8	More Details
CVE-2020-29007	The Score extension through 0.3.0 for MediaWiki has a remote code execution vulnerability due to improper sandboxing of the GNU LilyPond executable. This allows any user with an ability to edit articles (potentially including unauthenticated anonymous users) to execute arbitrary Scheme or shell code by using crafted {{Image data to generate musical scores containing malicious code.	9.8	More Details
CVE-2018-17452	An issue was discovered in GitLab Community and Enterprise Edition before 11.1.7, 11.2.x before 11.2.4, and 11.3.x before 11.3.1. There is Server-Side Request Forgery (SSRF) via a loopback address to the validate_localhost function in url_blocker.rb.	9.8	More Details
CVE-2022-34128	The Cartography (aka positions) plugin before 6.0.1 for GLPI allows remote code execution via PHP code in the POST data to front/upload.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33990	Liferay Portal 6.2.5 allows Command=FileUpload&Type=File&CurrentFolder=/ requests when frmfolders.html exists. NOTE: The vendor disputes this issue because the exploit reference link only shows frmfolders.html is accessible and does not demonstrate how an unauthorized user can upload a file.	9.8	More Details
CVE-2022-2525	Improper Restriction of Excessive Authentication Attempts in GitHub repository janeczku/calibre-web prior to 0.6.20.	9.8	More Details
CVE-2023-26463	strongSwan 5.9.8 and 5.9.9 potentially allows remote code execution because it uses a variable named "public" for two different purposes within the same function. There is initially incorrect access control, later followed by an expired pointer dereference. One attack vector is sending an untrusted client certificate during EAP-TLS. A server is affected only if it loads plugins that implement TLS-based EAP methods (EAP-TLS, EAP-TTLS, EAP-PEAP, or EAP-TNC). This is fixed in 5.9.10.	9.8	More Details
CVE-2021-46880	x509/x509_verify.c in LibreSSL before 3.4.2, and OpenBSD before 7.0 errata 006, allows authentication bypass because an error for an unverified certificate chain is sometimes discarded.	9.8	More Details
CVE-2023-27032	Prestashop advancedpopupcreator v1.1.21 to v1.1.24 was discovered to contain a SQL injection vulnerability via the component AdvancedPopup::getPopups().	9.8	More Details
CVE-2023-29199	There exists a vulnerability in source code transformer (exception sanitization logic) of vm2 for versions up to 3.9.15, allowing attackers to bypass `handleException()` and leak unsanitized host exceptions which can be used to escape the sandbox and run arbitrary code in host context. A threat actor can bypass the sandbox protections to gain remote code execution rights on the host running the sandbox. This vulnerability was patched in the release of version `3.9.16` of `vm2`.	9.8	More Details
CVE-2023-30547	vm2 is a sandbox that can run untrusted code with whitelisted Node's built-in modules. There exists a vulnerability in exception sanitization of vm2 for versions up to 3.9.16, allowing attackers to raise an unsanitized host exception inside `handleException()` which can be used to escape the sandbox and run arbitrary code in host context. This vulnerability was patched in the release of version `3.9.17` of `vm2`. There are no known workarounds for this vulnerability. Users are advised to upgrade.	9.8	More Details
CVE-2023-29412	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability exists that could cause remote code execution when manipulating internal methods through Java RMI interface.	9.8	More Details
CVE-2023-29411	A CWE-306: Missing Authentication for Critical Function vulnerability exists that could allow changes to administrative credentials, leading to potential remote code execution without requiring prior authentication on the Java RMI interface.	9.8	More Details
CVE-2022-46640	Nanoleaf Desktop App before v1.3.1 was discovered to contain a command injection vulnerability which is exploited via a crafted HTTP request.	9.8	More Details
CVE-2021-40507	An issue was discovered in the ALU unit of the OR1200 (aka OpenRISC 1200) processor 2011-09-10 through 2015-11-11. The overflow flag is not being updated correctly for the subtract instruction, which results in an incorrect value in the overflow flag. Any software that relies on this flag may experience corruption in execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40506	An issue was discovered in the ALU unit of the OR1200 (aka OpenRISC 1200) processor 2011-09-10 through 2015-11-11. The overflow flag is not being updated for the msb and mac instructions, which results in an incorrect value in the overflow flag. Any software that relies on this flag may experience corruption in execution.	9.8	More Details
CVE-2023-2138	Use of Hard-coded Credentials in GitHub repository nuxtlabs/github-module prior to 1.6.2.	9.8	More Details
CVE-2023-24501	Electra Central AC unit – Hardcoded Credentials in unspecified code used by the unit.	9.8	More Details
CVE-2023-24831	Improper Authentication vulnerability in Apache Software Foundation Apache IoTDB.This issue affects Apache IoTDB Grafana Connector: from 0.13.0 through 0.13.3. Attackers could login without authorization. This is fixed in 0.13.4.	9.8	More Details
CVE-2021-33797	Buffer-overflow in jsdtoa.c in Artifex MuJS in versions 1.0.1 to 1.1.1. An integer overflow happens when js_strtod() reads in floating point exponent, which leads to a buffer overflow in the pointer *d.	9.8	More Details
CVE-2023-29665	D-Link DIR823G_V1.0.2B05 was discovered to contain a stack overflow via the NewPassword parameters in SetPasswdSettings.	9.8	More Details
CVE-2023-1873	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Faturamatik Bircard allows SQL Injection.This issue affects Bircard: before 23.04.05.	9.8	More Details
CVE-2023-27844	SQL injection vulnerability found in PrestaShopleurlrewrite v.1.0 and before allow a remote attacker to gain privileges via the Dispatcher::getController component.	9.8	More Details
CVE-2023-1723	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Veragroup Mobile Assistant allows SQL Injection.This issue affects Mobile Assistant: before 21.S.2343.	9.8	More Details
CVE-2023-30771	Incorrect Authorization vulnerability in Apache Software Foundation Apache IoTDB.This issue affects the iotdb-web-workbench component on 0.13.3. iotdb-web-workbench is an optional component of IoTDB, providing a web console of the database. This problem is fixed from version 0.13.4 of iotdb-web-workbench onwards.	9.8	More Details
CVE-2023-27654	An issue found in WHOv.1.0.28, v.1.0.30, v.1.0.32 allows an attacker to cause a escalation of privileges via the TTMultiProvider component.	9.8	More Details
CVE-2023-2027	The ZM Ajax Login & Register plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 2.0.2. This is due to insufficient verification on the user being supplied during a Facebook login through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the username.	9.8	More Details
CVE-2022-3748	Improper Authorization vulnerability in ForgeRock Inc. Access Management allows Authentication Bypass. This issue affects Access Management: from 6.5.0 through 7.2.0.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27779	AM Presencia v3.7.3 was discovered to contain a SQL injection vulnerability via the user parameter in the login form.	9.8	More Details
CVE-2023-1863	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Eskom Water Metering Software allows Command Line Execution through SQL Injection.This issue affects Water Metering Software: before 23.04.06.	9.8	More Details
CVE-2023-29805	WFS-SR03 v1.0.3 was discovered to contain a command injection vulnerability via the pro_stor_canceltrans_handler_part_19 function.	9.8	More Details
CVE-2023-26918	Diasoft File Replication Pro 7.5.0 allows attackers to escalate privileges by replacing a legitimate file with a Trojan horse that will be executed as LocalSystem. This occurs because %ProgramFiles%\FileReplicationPro allows Everyone:(F) access.	9.8	More Details
CVE-2023-27748	BlackVue DR750-2CH LTE v.1.012_2022.10.26 does not employ authenticity check for uploaded firmware. This can allow attackers to upload crafted firmware which contains backdoors and enables arbitrary code execution.	9.8	More Details
CVE-2023-27746	BlackVue DR750-2CH LTE v.1.012_2022.10.26 was discovered to contain a weak default passphrase which can be easily cracked via a brute force attack if the WPA2 handshake is intercepted.	9.8	More Details
CVE-2023-27667	Auto Dealer Management System v1.0 was discovered to contain a SQL injection vulnerability.	9.8	More Details
CVE-2023-29598	lmxcms v1.4.1 was discovered to contain a SQL injection vulnerability via the setbook parameter at index.php.	9.8	More Details
CVE-2023-1617	Improper Authentication vulnerability in B&R Industrial Automation B&R VC4 (VNC-Server modules). This vulnerability may allow an unauthenticated network-based attacker to bypass the authentication mechanism of the VC4 visualization on affected devices. The impact of this vulnerability depends on the functionality provided in the visualization. This issue affects B&R VC4: from 3.* through 3.96.7, from 4.0* through 4.06.7, from 4.1* through 4.16.3, from 4.2* through 4.26.8, from 4.3* through 4.34.6, from 4.4* through 4.45.1, from 4.5* through 4.45.3, from 4.7* through 4.72.9.	9.8	More Details
CVE-2022-33259	Memory corruption due to buffer copy without checking the size of input in modem while decoding raw SMS received.	9.8	More Details
CVE-2022-33211	memory corruption in modem due to improper check while calculating size of serialized CoAP message	9.8	More Details
CVE-2022-25745	Memory corruption in modem due to improper input validation while handling the incoming CoAP message	9.8	More Details
CVE-2022-25740	Memory corruption in modem due to buffer overwrite while building an IPv6 multicast address based on the MAC address of the iface	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25678	Memory correction in modem due to buffer overwrite during coap connection	9.8	More Details
CVE-2023-28121	An issue in WooCommerce Payments plugin for WordPress (versions 5.6.1 and lower) allows an unauthenticated attacker to send requests on behalf of an elevated user, like administrator. This allows a remote, unauthenticated attacker to gain admin access on a site that has the affected version of the plugin activated.	9.8	More Details
CVE-2022-47027	Timmystudios Fast Typing Keyboard v1.275.1.162 allows unauthorized apps to overwrite arbitrary files in its internal storage via a dictionary traversal vulnerability and achieve arbitrary code execution.	9.8	More Details
CVE-2023-29622	Purchase Order Management v1.0 was discovered to contain a SQL injection vulnerability via the password parameter at /purchase_order/admin/login.php.	9.8	More Details
CVE-2023-28004	A CWE-129: Improper validation of an array index vulnerability exists where a specially crafted Ethernet request could result in denial of service or remote code execution.	9.8	More Details
CVE-2023-29798	TOTOLINK X18 V9.1.0cu.2024_B20220329 was discovered to contain a command injection vulnerability via the command parameter in the setTracerouteCfg function.	9.8	More Details
CVE-2023-29801	TOTOLINK X18 V9.1.0cu.2024_B20220329 was discovered to contain multiple command injection vulnerabilities via the rtLogEnabled and rtLogServer parameters in the setSyslogCfg function.	9.8	More Details
CVE-2023-27648	Directory Traversal vulnerability found in T-ME Studios Change Color of Keypad v.1.275.1.277 allows a remote attacker to execute arbitrary code via the dex file in the internal storage.	9.8	More Details
CVE-2023-29799	TOTOLINK X18 V9.1.0cu.2024_B20220329 was discovered to contain a command injection vulnerability via the hostname parameter in the setOpModeCfg function.	9.8	More Details
CVE-2023-29802	TOTOLINK X18 V9.1.0cu.2024_B20220329 was discovered to contain a command injection vulnerability via the ip parameter in the setDiagnosisCfg function.	9.8	More Details
CVE-2023-29800	TOTOLINK X18 V9.1.0cu.2024_B20220329 was discovered to contain a command injection vulnerability via the FileName parameter in the UploadFirmwareFile function.	9.8	More Details
CVE-2023-1833	Authentication Bypass by Primary Weakness vulnerability in DTS Electronics Redline Router firmware allows Authentication Bypass.This issue affects Redline Router: before 7.17.	9.8	More Details
CVE-2023-1803	Authentication Bypass by Alternate Name vulnerability in DTS Electronics Redline Router firmware allows Authentication Bypass.This issue affects Redline Router: before 7.17.	9.8	More Details
CVE-2022-45174	An issue was discovered in LIVEBOX Collaboration vDesk through v018. A Bypass of Two-Factor Authentication for SAML Users can occur under the /login/backup_code endpoint and the /api/v1/vdeskintegration/challenge endpoint. The correctness of the TOTP is not checked properly, and can be bypassed by passing any string as the backup code.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29803	TOTOLINK X18 V9.1.0cu.2024_B20220329 was discovered to contain a command injection vulnerability via the pid parameter in the disconnectVPN function.	9.8	More Details
CVE-2022-45173	An issue was discovered in LIVEBOX Collaboration vDesk through v018. A Bypass of Two-Factor Authentication can occur under the /api/v1/vdeskintegration/challenge endpoint. Because only the client-side verifies whether a check was successful, an attacker can modify the response, and fool the application into concluding that the TOTP was correct.	9.8	More Details
CVE-2023-28839	Shoppingfeed PrestaShop is an add-on to the PrestaShop ecommerce platform to synchronize data. The module Shoppingfeed for PrestaShop is vulnerable to SQL injection between version 1.4.0 and 1.8.2 due to a lack of input sanitization. This issue has been addressed in version 1.8.3. Users are advised to upgrade. There are no known workarounds for this issue.	9.4	More Details
CVE-2022-33231	Memory corruption due to double free in core while initializing the encryption key.	9.3	More Details
CVE-2022-33288	Memory corruption due to buffer copy without checking the size of input in Core while sending SCM command to get write protection information.	9.3	More Details
CVE-2022-33269	Memory corruption due to integer overflow or wraparound in Core while DDR memory assignment.	9.3	More Details
CVE-2023-24509	On affected modular platforms running Arista EOS equipped with both redundant supervisor modules and having the redundancy protocol configured with RPR or SSO, an existing unprivileged user can login to the standby supervisor as a root user, leading to a privilege escalation. Valid user credentials are required in order to exploit this vulnerability.	9.3	More Details
CVE-2023-28863	AMI MegaRAC SPx12 and SPx13 devices have Insufficient Verification of Data Authenticity.	9.1	More Details
CVE-2022-48312	The HwPCAssistant module has the out-of-bounds read/write vulnerability. Successful exploitation of this vulnerability may affect confidentiality and integrity.	9.1	More Details
CVE-2023-27812	bloofox v0.5.2 was discovered to contain an arbitrary file deletion vulnerability via the delete_file() function.	9.1	More Details
CVE-2023-29507	XWiki Commons are technical libraries common to several other top level XWiki projects. The Document script API returns directly a DocumentAuthors allowing to set any authors to the document, which in consequence can allow subsequent executions of scripts since this author is used for checking rights. The problem has been patched in XWiki 14.10 and 14.4.7 by returning a safe script API.	9.1	More Details
CVE-2023-30769	Vulnerability discovered is related to the peer-to-peer (p2p) communications, attackers can craft consensus messages, send it to individual nodes and take them offline. An attacker can crawl the network peers using getaddr message and attack the unpatched nodes.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29201	XWiki Commons are technical libraries common to several other top level XWiki projects. The "restricted" mode of the HTML cleaner in XWiki, introduced in version 4.2-milestone-1, only escaped `<script>` and `<style>`-tags but neither attributes that can be used to inject scripts nor other dangerous HTML tags like `<iframe>`. As a consequence, any code relying on this "restricted" mode for security is vulnerable to JavaScript injection ("cross-site scripting"/XSS). When a privileged user with programming rights visits such a comment in XWiki, the malicious JavaScript code is executed in the context of the user session. This allows server-side code execution with programming rights, impacting the confidentiality, integrity and availability of the XWiki instance. This problem has been patched in XWiki 14.6 RC1 with the introduction of a filter with allowed HTML elements and attributes that is enabled in restricted mode. There are no known workarounds apart from upgrading to a version including the fix.	9.0	More Details
CVE-2023-29213	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions of `org.xwiki.platform:xwiki-platform-logging-ui` it is possible to trick a user with programming rights into visiting a constructed url where e.g., by embedding an image with this URL in a document that is viewed by a user with programming rights which will evaluate an expression in the constructed url and execute it. This issue has been addressed in versions 13.10.11, 14.4.7, and 14.10. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.0	More Details
CVE-2023-27830	TightVNC before v2.8.75 allows attackers to escalate privileges on the host operating system via replacing legitimate files with crafted files when executing a file transfer. This is due to the fact that TightVNC runs in the backend as a high-privileges account.	9.0	More Details
CVE-2023-29202	XWiki Commons are technical libraries common to several other top level XWiki projects. The RSS macro that is bundled in XWiki included the content of the feed items without any cleaning in the HTML output when the parameter `content` was set to `true`. This allowed arbitrary HTML and in particular also JavaScript injection and thus cross-site scripting (XSS) by specifying an RSS feed with malicious content. With the interaction of a user with programming rights, this could be used to execute arbitrary actions in the wiki, including privilege escalation, remote code execution, information disclosure, modifying or deleting content and sabotaging the wiki. The issue has been patched in XWiki 14.6 RC1, the content of the feed is now properly cleaned before being displayed. As a workaround, if the RSS macro isn't used in the wiki, the macro can be uninstalled by deleting `WEB-INF/lib/xwiki-platform-rendering-macro-rss-XX.jar`, where `XX` is XWiki's version, in the web application's directory.	9.0	More Details
CVE-2023-29206	XWiki Commons are technical libraries common to several other top level XWiki projects. There was no check in the author of a JavaScript xobject or StyleSheet xobject added in a XWiki document, so until now it was possible for a user having only Edit Right to create such object and to craft a script allowing to perform some operations when executing by a user with appropriate rights. This has been patched in XWiki 14.9-rc-1 by only executing the script if the author of it has Script rights.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference

CVE Number	Description	Base Score	Reference
CVE-2023-29207	XWiki Commons are technical libraries common to several other top level XWiki projects. The Livetable Macro wasn't properly sanitizing column names, thus allowing the insertion of raw HTML code including JavaScript. This vulnerability was also exploitable via the Documents Macro that is included since XWiki 3.5M1 and doesn't require script rights, this can be demonstrated with the syntax `{{documents id="example" count="5" actions="false" columns="doc.title, before<script>alert(1)</script>after"/}}`. Therefore, this can also be exploited by users without script right and in comments. With the interaction of a user with more rights, this could be used to execute arbitrary actions in the wiki, including privilege escalation, remote code execution, information disclosure, modifying or deleting content. This has been patched in XWiki 14.9, 14.4.6, and 13.10.10.	8.9	More Details
CVE-2023-29508	XWiki Commons are technical libraries common to several other top level XWiki projects. A user without script rights can introduce a stored XSS by using the Live Data macro, if the last author of the content of the page has script rights. This has been patched in XWiki 14.10, 14.4.7, and 13.10.11.	8.9	More Details
CVE-2023-2105	Session Fixation in GitHub repository alextselegidis/easyappointments prior to 1.5.0.	8.8	More Details
CVE-2023-25548	A CWE-863: Incorrect Authorization vulnerability exists that could allow access to device credentials on specific DCE endpoints not being properly secured when a hacker is using a low privileged user. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior)	8.8	More Details
CVE-2023-25547	A CWE-863: Incorrect Authorization vulnerability exists that could allow remote code execution on upload and install packages when a hacker is using a low privileged user account. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior)	8.8	More Details
CVE-2021-45464	kvmtool through 39181fc allows an out-of-bounds write, related to virtio/balloon.c and virtio/pci.c. This allows a guest OS user to execute arbitrary code on the host machine.	8.8	More Details
CVE-2023-2033	Type confusion in V8 in Google Chrome prior to 112.0.5615.121 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-1109	In Phoenix Contacts ENERGY AXC PU Web service an authenticated restricted user of the web frontend can access, read, write and create files throughout the file system using specially crafted URLs via the upload and download functionality of the web service. This may lead to full control of the service.	8.8	More Details
CVE-2022-38841	Linksys AX3200 1.1.00 is vulnerable to OS command injection by authenticated users via shell metacharacters to the diagnostics traceroute page.	8.8	More Details
CVE-2023-27755	go-bbs v1 was discovered to contain an arbitrary file download vulnerability via the component /api/v1/download.	8.8	More Details
CVE-2023-29597	bloofox v0.5.2 was discovered to contain a SQL injection vulnerability via the component /index.php?mode=content&page=pages&action=edit&eid=1.	8.8	More Details
CVE-2023-22294	Privilege escalation in Tribe29 Checkmk Appliance before 1.6.4 allows authenticated site users to escalate privileges via incorrectly set permissions.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29804	WFS-SR03 v1.0.3 was discovered to contain a command injection vulnerability via the sys_smb_pwdmod function.	8.8	More Details
CVE-2022-45030	A SQL injection vulnerability in rConfig 3.9.7 exists via lib/ajaxHandlers/ajaxCompareGetCmdDates.php?command= (this may interact with secure-file-priv).	8.8	More Details
CVE-2023-22951	An issue was discovered in TigerGraph Enterprise Free Edition 3.x. It creates an authentication token for internal systems use. This token can be read from the configuration file. Using this token on the REST API provides an attacker with anonymous admin-level privileges on all REST API endpoints.	8.8	More Details
CVE-2022-45178	An issue was discovered in LIVEBOX Collaboration vDesk through v018. Broken Access Control exists under the /api/v1/vdeskintegration/saml/user/createorupdate endpoint, the /settings/guest-settings endpoint, the /settings/samlusers-settings endpoint, and the /settings/users-settings endpoint. A malicious user (already logged in as a SAML User) is able to achieve privilege escalation from a low-privilege user (FGM user) to an administrative user (GGU user), including the administrator, or create new users even without an admin role.	8.8	More Details
CVE-2023-29584	mp4v2 v2.0.0 was discovered to contain a heap buffer overflow via the MP4GetVideoProfileLevel function at /src/mp4.cpp.	8.8	More Details
CVE-2023-2034	Unrestricted Upload of File with Dangerous Type in GitHub repository froxlor/froxlor prior to 2.0.14.	8.8	More Details
CVE-2023-29621	Purchase Order Management v1.0 was discovered to contain an arbitrary file upload vulnerability which allows attackers to execute arbitrary code via a crafted file uploaded to the server.	8.8	More Details
CVE-2023-29625	Employee Performance Evaluation System v1.0 was discovered to contain an arbitrary file upload vulnerability which allows attackers to execute arbitrary code via a crafted file uploaded to the server.	8.8	More Details
CVE-2023-29627	Online Pizza Ordering v1.0 was discovered to contain an arbitrary file upload vulnerability which allows attackers to execute arbitrary code via a crafted file uploaded to the server.	8.8	More Details
CVE-2023-0765	The Gallery by BestWebSoft WordPress plugin before 4.7.0 does not properly escape values used in SQL queries, leading to an Blind SQL Injection vulnerability. The attacker must have at least the privileges of an Author, and the vendor's Slider plugin (https://wordpress.org/plugins/slider-bws/) must also be installed for this vulnerability to be exploitable.	8.8	More Details
CVE-2023-2017	Server-side Template Injection (SSTI) in Shopware 6 (<= v6.4.20.0, v6.5.0.0-rc1 <= v6.5.0.0-rc4), affecting both shopware/core and shopware/platform GitHub repositories, allows remote attackers with access to a Twig environment without the Sandbox extension to bypass the validation checks in `Shopware\Core\Framework\Adapter\Twig\SecurityExtension` and call any arbitrary PHP function and thus execute arbitrary code/commands via usage of fully-qualified names, supplied as array of strings, when referencing callables. Users are advised to upgrade to v6.4.20.1 to resolve this issue. This is a bypass of CVE-2023-22731.	8.8	More Details
CVE-2023-30525	A cross-site request forgery (CSRF) vulnerability in Jenkins Report Portal Plugin 0.5 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified bearer token authentication.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27976	A CWE-668: Exposure of Resource to Wrong Sphere vulnerability exists that could cause remote code execution when a valid user visits a malicious link provided through the web endpoints. Affected Products: EcoStruxure Control Expert (V15.1 and above)	8.8	More Details
CVE-2023-27826	SeowonIntech SWC 5100W WIMAX Bootloader 1.18.19.0, HW 0.0.7.0, and FW 1.11.0.1, 1.9.9.4 are vulnerable to OS Command Injection. which allows attackers to take over the system with root privilege by abusing doSystem() function.	8.8	More Details
CVE-2018-17451	An issue was discovered in GitLab Community and Enterprise Edition before 11.1.7, 11.2.x before 11.2.4, and 11.3.x before 11.3.1. There is Cross Site Request Forgery (CSRF) in the Slack integration for issuing slash commands.	8.8	More Details
CVE-2021-41612	An issue was discovered in the ALU unit of the OpenRISC mor1kx processor. The carry flag is not being updated correctly for the subtract instruction, which results in an incorrect value of the carry flag. Any software that relies on this flag may experience corruption in execution.	8.8	More Details
CVE-2023-28983	An OS Command Injection vulnerability in gRPC Network Operations Interface (gNOI) server module of Juniper Networks Junos OS Evolved allows an authenticated, low privileged, network based attacker to inject shell commands and execute code. This issue affects Juniper Networks Junos OS Evolved 21.4 version 21.4R1-EVO and later versions prior to 22.1R1-EVO.	8.8	More Details
CVE-2023-27216	An issue found in D-Link DSL-3782 v.1.03 allows remote authenticated users to execute arbitrary code as root via the network settings page.	8.8	More Details
CVE-2023-29193	SpiceDB is an open source, Google Zanzibar-inspired, database system for creating and managing security-critical application permissions. The `spicedb serve` command contains a flag named `--grpc-preshared-key` which is used to protect the gRPC API from being accessed by unauthorized requests. The values of this flag are to be considered sensitive, secret data. The `/debug/pprof/cmdline` endpoint served by the metrics service (defaulting running on port `9090`) reveals the command-line flags provided for debugging purposes. If a password is set via the `--grpc-preshared-key` then the key is revealed by this endpoint along with any other flags provided to the SpiceDB binary. This issue has been fixed in version 1.19.1. ### Impact All deployments abiding by the recommended best practices for production usage are **NOT affected**: - Authzed's SpiceDB Serverless - Authzed's SpiceDB Dedicated - SpiceDB Operator Users configuring SpiceDB via environment variables are **NOT affected**. Users **MAY be affected** if they expose their metrics port to an untrusted network and are configuring `--grpc-preshared-key` via command-line flag. ### Patches TODO ### Workarounds To workaround this issue you can do one of the following: - Configure the preshared key via an environment variable (e.g. `SPICEDB_GRPC_PRESHARED_KEY=yoursecret spicedb serve`) - Reconfigure the `--metrics-addr` flag to bind to a trusted network (e.g. `--metrics-addr=localhost:9090`) - Disable the metrics service via the flag (e.g. `--metrics-enabled=false`) - Adopt one of the recommended deployment models: [Authzed's managed services](https://authzed.com/pricing) or the [SpiceDB Operator](https://github.com/authzed/spicedb-operator) ### References - [GitHub Security Advisory issued for SpiceDB](https://github.com/authzed/spicedb/security/advisories/GHSA-cjr9-mr35-7xh6) - [Go issue #22085](https://github.com/golang/go/issues/22085) for documenting the risks of exposing pprof to the internet - [Go issue #42834](https://github.com/golang/go/issues/42834) discusses preventing pprof registration to the default serve mux - [semgrep rule go.lang.security.audit.net.pprof.pprof-debug-exposure](https://semgrep.dev/r?q=go.lang.security.audit.net.pprof) checks for a variation of this issue ### Credit We'd like to thank Amit Laish, a security researcher at GE Vernova for responsibly disclosing this vulnerability.	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17354	LilyPond before 2.24 allows attackers to bypass the -dsafe protection mechanism via output-def-lookup or output-def-scope, as demonstrated by dangerous Scheme code in a .ly file that causes arbitrary code execution during conversion to a different file format. NOTE: in 2.24 and later versions, safe mode is removed, and the product no longer tries to block code execution when external files are used.	8.6	More Details
CVE-2022-33282	Memory corruption in Automotive Multimedia due to integer overflow to buffer overflow during IOCTL calls in video playback.	8.4	More Details
CVE-2023-21630	Memory Corruption in Multimedia Framework due to integer overflow when synx bind is called along with synx signal.	8.4	More Details
CVE-2022-40532	Memory corruption due to integer overflow or wraparound in WLAN while sending WMI cmd from host to target.	8.4	More Details
CVE-2023-21923	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences InForm. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Health Sciences InForm accessible data as well as unauthorized access to critical data or complete access to all Oracle Health Sciences InForm accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Health Sciences InForm. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L).	8.3	More Details
CVE-2023-25556	A CWE-287: Improper Authentication vulnerability exists that could allow a device to be compromised when a key of less than seven digits is entered and the attacker has access to the KNX installation.	8.3	More Details
CVE-2022-47605	Auth. SQL Injection') vulnerability in Kunal Nagar Custom 404 Pro plugin <= 3.7.0 versions.	8.3	More Details
CVE-2022-33258	Information disclosure due to buffer over-read in modem while reading configuration parameters.	8.2	More Details
CVE-2022-25726	Information disclosure in modem data due to array out of bound access while handling the incoming DNS response packet	8.2	More Details
CVE-2022-25730	Information disclosure in modem due to improper check of IP type while processing DNS server query	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28960	An Incorrect Permission Assignment for Critical Resource vulnerability in Juniper Networks Junos OS Evolved allows a local, authenticated low-privileged attacker to copy potentially malicious files into an existing Docker container on the local system. A follow-on administrator could then inadvertently start the Docker container leading to the malicious files being executed as root. This issue only affects systems with Docker configured and enabled, which is not enabled by default. Systems without Docker started are not vulnerable to this issue. This issue affects Juniper Networks Junos OS Evolved: 20.4 versions prior to 20.4R3-S5-EVO; 21.2 versions prior to 21.2R3-EVO; 21.3 versions prior to 21.3R3-EVO; 21.4 versions prior to 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 19.2R1-EVO.	8.2	More Details
CVE-2022-33228	Information disclosure sue to buffer over-read in modem while processing ipv6 packet with hop-by-hop or destination option in header.	8.2	More Details
CVE-2022-33291	Information disclosure in Modem due to buffer over-read while receiving a IP header with malformed length.	8.2	More Details
CVE-2022-33222	Information disclosure due to buffer over-read while parsing DNS response packets in Modem.	8.2	More Details
CVE-2022-25747	Information disclosure in modem due to improper input validation during parsing of upcoming CoAP message	8.2	More Details
CVE-2022-33287	Information disclosure in Modem due to buffer over-read while getting length of Unfragmented headers in an IPv6 packet.	8.2	More Details
CVE-2022-33295	Information disclosure in Modem due to buffer over-read while parsing the wms message received given the buffer and its length.	8.2	More Details
CVE-2023-21990	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details
CVE-2022-40503	Information disclosure due to buffer over-read in Bluetooth Host while A2DP streaming.	8.2	More Details
CVE-2023-25552	A CWE-862: Missing Authorization vulnerability exists that could allow viewing of unauthorized content, changes or deleting of content, or performing unauthorized functions when tampering the Device File Transfer settings on DCE endpoints. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior)	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29018	The OpenFeature Operator allows users to expose feature flags to applications. Assuming the pre-existence of a vulnerability that allows for arbitrary code execution, an attacker could leverage the lax permissions configured on `open-feature-operator-controller-manager` to escalate the privileges of any SA in the cluster. The increased privileges could be used to modify cluster state, leading to DoS, or read sensitive data, including secrets. Version 0.2.32 mitigates this issue by restricting the resources the `open-feature-operator-controller-manager` can modify.	8.0	More Details
CVE-2022-45064	The SlingRequestDispatcher doesn't correctly implement the RequestDispatcher API resulting in a generic type of include-based cross-site scripting issues on the Apache Sling level. The vulnerability is exploitable by an attacker that is able to include a resource with specific content-type and control the include path (i.e. writing content). The impact of a successful attack is privilege escalation to administrative power. Please update to Apache Sling Engine >= 2.14.0 and enable the "Check Content-Type overrides" configuration option.	8.0	More Details
CVE-2023-26383	Adobe Substance 3D Stager version 2.0.1 (and earlier) is affected by a Stack-based Buffer Overflow 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-2023-21582	Adobe Digital Editions version 4.5.11.187303 (and earlier) is 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-2023-22235	InCopy versions 18.1 (and earlier), 17.4 (and earlier) are affected by a Use After Free 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-2023-29067	A maliciously crafted X_B file when parsed through Autodesk® AutoCAD® 2023 could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2023-26402	Adobe Substance 3D Stager version 2.0.1 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code 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-2023-26391	Adobe Substance 3D Stager version 2.0.1 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code 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-2023-26384	Adobe Substance 3D Stager version 2.0.1 (and earlier) is affected by a Use After Free 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-2023-26392	Adobe Substance 3D Stager version 2.0.1 (and earlier) is affected by a Use After Free 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-2023-25010	A malicious actor may convince a victim to open a malicious USD file that may trigger an uninitialized variable which may result in code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21948	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Core). The supported version that is affected is 10. 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. 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-2023-26389	Adobe Substance 3D Stager version 2.0.1 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code 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-2023-26393	Adobe Substance 3D Stager version 2.0.1 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code 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-2023-26390	Adobe Substance 3D Stager version 2.0.1 (and earlier) is affected by a Stack-based Buffer Overflow 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-2023-26394	Adobe Substance 3D Stager version 2.0.1 (and earlier) is affected by a Heap-based Buffer Overflow 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-2023-26388	Adobe Substance 3D Stager version 2.0.1 (and earlier) is affected by an Improper Input Validation 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-2023-26416	Adobe Substance 3D Designer version 12.4.0 (and earlier) is affected by a Heap-based Buffer Overflow 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-2023-26415	Adobe Substance 3D Designer version 12.4.0 (and earlier) is 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-2023-26414	Adobe Substance 3D Designer version 12.4.0 (and earlier) is affected by a Use After Free 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-2023-26413	Adobe Substance 3D Designer version 12.4.0 (and earlier) is affected by a Heap-based Buffer Overflow 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-2023-27915	A maliciously crafted X_B file when parsed through Autodesk® AutoCAD® 2023 could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2023-26412	Adobe Substance 3D Designer version 12.4.0 (and earlier) is affected by a Stack-based Buffer Overflow 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-2023-26411	Adobe Substance 3D Designer version 12.4.0 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code 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-2023-27914	A maliciously crafted X_B file when parsed through Autodesk® AutoCAD® 2023 can be used to write beyond the allocated buffer causing a Stack Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash or read sensitive data or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2023-27913	A maliciously crafted X_B file when parsed through Autodesk® AutoCAD® 2023 can be used to cause an Integer Overflow. A malicious actor can leverage this vulnerability to cause a crash or read sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2023-27912	A maliciously crafted X_B file when parsed through Autodesk® AutoCAD® 2023 can force an Out-of-Bound Read. A malicious actor can leverage this vulnerability to cause a crash or read sensitive data or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2023-26410	Adobe Substance 3D Designer version 12.4.0 (and earlier) is affected by a Use After Free 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-2023-26409	Adobe Substance 3D Designer version 12.4.0 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code 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-2023-26398	Adobe Substance 3D Designer version 12.4.0 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code 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-2023-21987	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	7.8	More Details
CVE-2023-1872	A use-after-free vulnerability in the Linux Kernel io_uring system can be exploited to achieve local privilege escalation. The io_file_get_fixed function lacks the presence of ctx->uring_lock which can lead to a Use-After-Free vulnerability due a race condition with fixed files getting unregistered. We recommend upgrading past commit da24142b1ef9fd5d36b76e36bab328a5b27523e8.	7.8	More Details
CVE-2023-27906	A malicious actor may convince a victim to open a malicious USD file that may trigger an out-of-bounds read vulnerability which may result in code execution.	7.8	More Details
CVE-2023-27907	A malicious actor may convince a victim to open a malicious USD file that may trigger an out-of-bounds write vulnerability which may result in code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26425	Adobe Acrobat Reader versions 23.001.20093 (and earlier) and 20.005.30441 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code 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-2023-28966	An Incorrect Default Permissions vulnerability in Juniper Networks Junos OS Evolved allows a low-privileged local attacker with shell access to modify existing files or execute commands as root. The issue is caused by improper file and directory permissions on certain system files, allowing an attacker with access to these files and folders to inject CLI commands as root. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S5-EVO; 21.2 versions prior to 21.2R3-EVO; 21.3 versions prior to 21.3R2-EVO.	7.8	More Details
CVE-2023-1829	A use-after-free vulnerability in the Linux Kernel traffic control index filter (tcindex) can be exploited to achieve local privilege escalation. The tcindex_delete function which does not properly deactivate filters in case of a perfect hashes while deleting the underlying structure which can later lead to double freeing the structure. A local attacker user can use this vulnerability to elevate its privileges to root. We recommend upgrading past commit 8c710f75256bb3cf05ac7b1672c82b92c43f3d28.	7.8	More Details
CVE-2023-25554	A CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability exists that allows a local privilege escalation on the appliance when a maliciously crafted Operating System command is entered on the device. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior)	7.8	More Details
CVE-2023-29491	ncurses before 6.4 20230408, when used by a setuid application, allows local users to trigger security-relevant memory corruption via malformed data in a terminfo database file that is found in $HOME/.terminfo or reached via the TERMINFO or TERM environment variable.	7.8	More Details
CVE-2023-27193	An issue found in DUALSPACE v.1.1.3 allows a local attacker to gain privileges via the key_ad_new_user_avoid_time field.	7.8	More Details
CVE-2023-26424	Adobe Acrobat Reader versions 23.001.20093 (and earlier) and 20.005.30441 (and earlier) are affected by a Use After Free 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-2023-22616	An issue was discovered in Insyde InsydeH2O with kernel 5.2 through 5.5. The Save State register is not checked before use. The IhisiSmm driver does not check the value of a save state register before use. Due to insufficient input validation, an attacker can corrupt SMRAM.	7.8	More Details
CVE-2021-41614	An issue was discovered in the controller unit of the OpenRISC mor1kx processor. The read/write access permissions to the Exception Program Counter Register (EPCR) are not implemented correctly. User programs from an unauthorized privilege level can make read/write accesses to EPCR.	7.8	More Details
CVE-2023-27910	A user may be tricked into opening a malicious FBX file that may exploit a stack buffer overflow vulnerability in Autodesk® FBX® SDK 2020 or prior which may lead to code execution.	7.8	More Details
CVE-2023-26373	Adobe Dimension version 3.4.8 (and earlier) is 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-2023-26372	Adobe Dimension version 3.4.8 (and earlier) is 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-2023-26371	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code 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-2023-2008	A flaw was found in the Linux kernel's udmabuf device driver. The specific flaw exists within a fault handler. The issue results from the lack of proper validation of user-supplied data, which can result in a memory access past the end of an array. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the kernel.	7.8	More Details
CVE-2023-22670	A heap-based buffer overflow exists in the DXF file reading procedure in Open Design Alliance Drawings SDK before 2023.6. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of the length of user-supplied XRecord data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2023-27651	An issue found in Ego Studio SuperClean v.1.1.9 and v.1.1.5 allows an attacker to gain privileges via the update_info field of the _default_.xml file.	7.8	More Details
CVE-2023-22669	Parsing of DWG files in Open Design Alliance Drawings SDK before 2023.6 lacks proper validation of the length of user-supplied XRecord data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2023-27911	A user may be tricked into opening a malicious FBX file that may exploit a heap buffer overflow vulnerability in Autodesk® FBX® SDK 2020 or prior which may lead to code execution.	7.8	More Details
CVE-2023-2091	A vulnerability classified as critical was found in KylinSoft youker-assistant on KylinOS. Affected by this vulnerability is the function adjust_cpufreq_scaling_governer. The manipulation leads to os command injection. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. Upgrading to version 3.1.4.13 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-226099.	7.8	More Details
CVE-2023-26419	Adobe Acrobat Reader versions 23.001.20093 (and earlier) and 20.005.30441 (and earlier) are affected by a Use After Free 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-2023-26417	Adobe Acrobat Reader versions 23.001.20093 (and earlier) and 20.005.30441 (and earlier) are affected by a Use After Free 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-2023-26408	Adobe Acrobat Reader versions 23.001.20093 (and earlier) and 20.005.30441 (and earlier) are affected by an Improper Access Control 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-2023-26420	Adobe Acrobat Reader versions 23.001.20093 (and earlier) and 20.005.30441 (and earlier) are affected by a Use After Free 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-2023-26407	Adobe Acrobat Reader versions 23.001.20093 (and earlier) and 20.005.30441 (and earlier) are affected by an Improper Input Validation 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-2023-26406	Adobe Acrobat Reader versions 23.001.20093 (and earlier) and 20.005.30441 (and earlier) are affected by an Improper Access Control 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-2023-26405	Adobe Acrobat Reader versions 23.001.20093 (and earlier) and 20.005.30441 (and earlier) are affected by an Improper Input Validation 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-2023-27909	An Out-Of-Bounds Write Vulnerability in Autodesk® FBX® SDK version 2020 or prior may lead to code execution through maliciously crafted FBX files or information disclosure.	7.8	More Details
CVE-2023-26421	Adobe Acrobat Reader versions 23.001.20093 (and earlier) and 20.005.30441 (and earlier) are affected by an Integer Underflow or Wraparound 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-2023-26396	Adobe Acrobat Reader versions 23.001.20093 (and earlier) and 20.005.30441 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation 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-2023-26422	Adobe Acrobat Reader versions 23.001.20093 (and earlier) and 20.005.30441 (and earlier) are affected by a Use After Free 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-2023-26395	Adobe Acrobat Reader versions 23.001.20093 (and earlier) and 20.005.30441 (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-2023-26423	Adobe Acrobat Reader versions 23.001.20093 (and earlier) and 20.005.30441 (and earlier) are affected by a Use After Free 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-2023-26418	Adobe Acrobat Reader versions 23.001.20093 (and earlier) and 20.005.30441 (and earlier) are affected by a Use After Free 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-2023-21985	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Utility). Supported versions that are affected are 10 and 11. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Solaris, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Solaris. CVSS 3.1 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H).	7.7	More Details
CVE-2023-1326	A privilege escalation attack was found in apport-cli 2.26.0 and earlier which is similar to CVE-2023-26604. If a system is specially configured to allow unprivileged users to run sudo apport-cli, less is configured as the pager, and the terminal size can be set: a local attacker can escalate privilege. It is extremely unlikely that a system administrator would configure sudo to allow unprivileged users to perform this class of exploit.	7.7	More Details
CVE-2022-43376	A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause code and session manipulation when malicious code is inserted into the browser. Affected Products: NetBotz 4 - 355/450/455/550/570 (V4.7.0 and prior)	7.6	More Details
CVE-2023-27643	An issue found in POWERAMP 925-bundle-play and Poweramp 954-uni allows a remote attacker to cause a denial of service via the Rescan button in Queue and Select Folders button in Library	7.5	More Details
CVE-2023-29850	SENAYAN Library Management System (SLiMS) Bulian v9.5.2 does not strip exif data from uploaded images. This allows attackers to obtain information such as the user's geolocation and device information.	7.5	More Details
CVE-2023-26756	The login page of Revive Adserver v5.4.1 is vulnerable to brute force attacks. NOTE: The vendor's position is that this is effectively mitigated by rate limits and password-quality features.	7.5	More Details
CVE-2023-27649	SQL injection vulnerability found in Trusted Tools Free Music v.2.1.0.47, v.2.0.0.46, v.1.9.1.45, v.1.8.2.43 allows a remote attacker to cause a denial of service via the search history table	7.5	More Details
CVE-2021-43612	In lldpd before 1.0.13, when decoding SONMP packets in the sonmp_decode function, it's possible to trigger an out-of-bounds heap read via short SONMP packets.	7.5	More Details
CVE-2023-21964	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 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 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2023-21979	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server 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 Number	Description	Base Score	Reference
CVE-2023-26969	Atropim 1.5.26 is vulnerable to Directory Traversal.	7.5	More Details
CVE-2023-1285	Signal Handler Race Condition vulnerability in Mitsubishi Electric India GC-ENET-COM whose first 2 digits of 11-digit serial number of unit are "16" allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition in Ethernet communication by sending a large number of specially crafted packets to any UDP port when GC-ENET-COM is configured as a Modbus TCP Server. The communication resumes only when the power of the main unit is turned off and on or when the GC-ENET-COM is hot-swapped from the main unit.	7.5	More Details
CVE-2023-28982	A Missing Release of Memory after Effective Lifetime vulnerability in the routing protocol daemon of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network based attacker to cause a Denial of Service (DoS). In a BGP rib sharding scenario, when an attribute of an active BGP route is updated memory will leak. As rpd memory usage increases over time the rpd process will eventually run out of memory, crash, and restart. The memory utilization can be monitored with the following CLI commands: show task memory show system processes extensive | match rpd This issue affects: Juniper Networks Junos OS 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved 20.3-EVO version 20.3R1-EVO and later versions; 20.4-EVO versions prior to 20.4R3-S6-EVO; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO.	7.5	More Details
CVE-2023-29626	Yoga Class Registration System 1.0 was discovered to contain a SQL injection vulnerability via the cid parameter at /admin/login.php.	7.5	More Details
CVE-2023-27653	An issue found in WHOv.1.0.28, v.1.0.30, v.1.0.32 allows an attacker to cause a denial of service via the SharedPreference files.	7.5	More Details
CVE-2023-21912	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 5.7.41 and prior and 8.0.30 and prior. Easily exploitable vulnerability allows unauthenticated 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 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2023-29208	XWiki Commons are technical libraries common to several other top level XWiki projects. Rights added to a document are not taken into account for viewing it once it's deleted. Note that this vulnerability only impact deleted documents that where containing view rights: the view rights provided on a space of a deleted document are properly checked. The problem has been patched in XWiki 14.10 by checking the rights of current user: only admin and deleter of the document are allowed to view it.	7.5	More Details
CVE-2023-1874	The WP Data Access plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 5.3.7. This is due to a lack of authorization checks on the multiple_roles_update function. This makes it possible for authenticated attackers, with minimal permissions such as a subscriber, to modify their user role by supplying the 'wpda_role[]' parameter during a profile update. This requires the 'Enable role management' setting to be enabled for the site.	7.5	More Details
CVE-2023-30637	Baidu braft 1.1.2 has a memory leak related to use of the new operator in example/atomic/atomic_server. NOTE: installations with brpc-0.14.0 and later are unaffected.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27747	BlackVue DR750-2CH LTE v.1.012_2022.10.26 does not employ authentication in its web server. This vulnerability allows attackers to access sensitive information such as configurations and recordings.	7.5	More Details
CVE-2023-30636	TiKV 6.1.2 allows remote attackers to cause a denial of service (fatal error, with RpcStatus UNAVAILABLE for "not leader") upon an attempt to start a node in a situation where the context deadline is exceeded	7.5	More Details
CVE-2021-36520	A SQL injection vulnerability in I-Tech Trainsmart r1044 exists via a evaluation/assign-evaluation?id= URI.	7.5	More Details
CVE-2023-30635	TiKV 6.1.2 allows remote attackers to cause a denial of service (fatal error) upon an attempt to get a timestamp from the Placement Driver.	7.5	More Details
CVE-2021-39295	In OpenBMC 2.9, crafted IPMI messages allow an attacker to cause a denial of service to the BMC via the netipmid (IPMI lan+) interface.	7.5	More Details
CVE-2022-34127	The Managentities plugin before 4.0.2 for GLPI allows reading local files via directory traversal in the inc/cri.class.php file parameter.	7.5	More Details
CVE-2023-30514	Jenkins Azure Key Vault Plugin 187.va_cd5fecd198a_ and earlier does not properly mask (i.e., replace with asterisks) credentials in the build log when push mode for durable task logging is enabled.	7.5	More Details
CVE-2022-34126	The Activity plugin before 3.1.1 for GLPI allows reading local files via directory traversal in the front/cra.send.php file parameter.	7.5	More Details
CVE-2018-17449	An issue was discovered in GitLab Community and Enterprise Edition before 11.1.7, 11.2.x before 11.2.4, and 11.3.x before 11.3.1. Remote attackers could obtain sensitive information about issues, comments, and project titles via events API insecure direct object reference.	7.5	More Details
CVE-2023-21996	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP 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 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2023-24500	Electra Central AC unit – Adjacent attacker may cause the unit to load unauthorized FW.	7.5	More Details
CVE-2023-24502	Electra Central AC unit – The unit opens an AP with an easily calculated password.	7.5	More Details
CVE-2023-24503	Electra Central AC unit – Adjacent attacker may cause the unit to load unauthorized FW.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24504	Electra Central AC unit – Adjacent attacker may cause the unit to connect to unauthorized update server.	7.5	More Details
CVE-2022-37255	TP-Link Tapo C310 1.3.0 devices allow access to the RTSP video feed via credentials of User --- and Password TPL075526460603.	7.5	More Details
CVE-2023-28964	An Improper Handling of Length Parameter Inconsistency vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a network based, unauthenticated attacker to cause an RPD crash leading to a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. Upon receipt of a malformed BGP flowspec update, RPD will crash resulting in a Denial of Service. This issue affects Juniper Networks Junos OS: All versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2; Juniper Networks Junos OS Evolved: All versions prior to 20.1R3-EVO; 20.2 versions prior to 20.2R2-EVO; 20.3 versions prior to 20.3R2-EVO;	7.5	More Details
CVE-2023-28967	A Use of Uninitialized Resource vulnerability in the Border Gateway Protocol (BGP) software of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to send specific genuine BGP packets to a device configured with BGP to cause a Denial of Service (DoS) by crashing the Routing Protocol Daemon (rpd). This issue is triggered when the packets attempt to initiate a BGP connection before a BGP session is successfully established. Continued receipt of these specific BGP packets will cause a sustained Denial of Service condition. This issue is triggerable in both iBGP and eBGP deployments. This issue affects: Juniper Networks Junos OS 21.1 version 21.1R1 and later versions prior to 21.1R3-S5; 21.2 version 21.2R1 and later versions prior to 21.2R3-S2; 21.3 version 21.3R1 and later 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. This issue does not affect Juniper Networks Junos OS versions prior to 21.1R1. This issue affects: Juniper Networks Junos OS Evolved 21.1-EVO version 21.1R1-EVO and later versions prior to 21.4R3-EVO; 22.1-EVO versions prior to 22.1R3-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.1R1-EVO.	7.5	More Details
CVE-2023-29887	A Local File inclusion vulnerability in test.php in spreadsheet-reader 0.5.11 allows remote attackers to include arbitrary files via the File parameter.	7.5	More Details
CVE-2023-21931	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server 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-2023-24607	Qt before 6.4.3 allows a denial of service via a crafted string when the SQL ODBC driver plugin is used and the size of SQLTCHAR is 4. The affected versions are 5.x before 5.15.13, 6.x before 6.2.8, and 6.3.x before 6.4.3.	7.5	More Details
CVE-2018-17455	An issue was discovered in GitLab Enterprise Edition before 11.1.7, 11.2.x before 11.2.4, and 11.3.x before 11.3.1. Attackers could obtain sensitive information about group names, avatars, LDAP settings, and descriptions via an insecure direct object reference to the "merge request approvals" feature.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43377	A CWE-307: Improper Restriction of Excessive Authentication Attempts vulnerability exists that could cause account takeover when a brute force attack is performed on the account. Affected Products: NetBotz 4 - 355/450/455/550/570 (V4.7.0 and prior)	7.5	More Details
CVE-2023-30513	Jenkins Kubernetes Plugin 3909.v1f2c633e8590 and earlier does not properly mask (i.e., replace with asterisks) credentials in the build log when push mode for durable task logging is enabled.	7.5	More Details
CVE-2022-47522	The IEEE 802.11 specifications through 802.11ax allow physically proximate attackers to intercept (possibly cleartext) target-destined frames by spoofing a target's MAC address, sending Power Save frames to the access point, and then sending other frames to the access point (such as authentication frames or re-association frames) to remove the target's original security context. This behavior occurs because the specifications do not require an access point to purge its transmit queue before removing a client's pairwise encryption key.	7.5	More Details
CVE-2023-24545	On affected platforms running Arista CloudEOS an issue in the Software Forwarding Engine (Sfe) can lead to a potential denial of service attack by sending malformed packets to the switch. This causes a leak of packet buffers and if enough malformed packets are received, the switch may eventually stop forwarding traffic.	7.5	More Details
CVE-2022-38840	cgi-bin/xmlstatus.cgi in Güralp MAN-EAM-0003 3.2.4 is vulnerable to an XML External Entity (XXE) issue via XML file upload, which leads to local file disclosure.	7.5	More Details
CVE-2023-22620	An issue was discovered in SecurePoint UTM before 12.2.5.1. The firewall's endpoint at /spcgi.cgi allows sessionid information disclosure via an invalid authentication attempt. This can afterwards be used to bypass the device's authentication and get access to the administrative interface.	7.5	More Details
CVE-2022-33294	Transient DOS in Modem due to NULL pointer dereference while receiving response of lwm2m registration/update/bootstrap request message.	7.5	More Details
CVE-2023-27772	libiec61850 v1.5.1 was discovered to contain a segmentation violation via the function ControlObjectClient_setOrigin() at /client/client_control.c.	7.5	More Details
CVE-2023-28976	An Improper Check for Unusual or Exceptional Conditions vulnerability in the packet forwarding engine (pfe) of Juniper Networks Junos OS on MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). If specific traffic is received on MX Series and its rate exceeds the respective DDoS protection limit the ingress PFE will crash and restart. Continued receipt of this traffic will create a sustained DoS condition. 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-S11; 20.2 versions prior to 20.2R3-S5; 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; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2.	7.5	More Details
CVE-2022-40946	On D-Link DIR-819 Firmware Version 1.06 Hardware Version A1 devices, it is possible to trigger a Denial of Service via the sys_token parameter in a cgi-bin/webproc?getpage=html/index.html request.	7.5	More Details
CVE-2023-29413	A CWE-306: Missing Authentication for Critical Function vulnerability exists that could cause Denial-of-Service when accessed by an unauthenticated user on the Schneider UPS Monitor service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-15472	An issue was discovered in GitLab Community and Enterprise Edition before 11.1.7, 11.2.x before 11.2.4, and 11.3.x before 11.3.1. The diff formatter using rouge can block for a long time in Sidekiq jobs without any timeout.	7.5	More Details
CVE-2022-47501	Arbitrary file reading vulnerability in Apache Software Foundation Apache OFBiz when using the Solr plugin. This is a pre-authentication attack. This issue affects Apache OFBiz: before 18.12.07.	7.5	More Details
CVE-2023-27705	APNG_Optimizer v1.4 was discovered to contain a buffer overflow via the component /apngopt/ubuntu.png.	7.5	More Details
CVE-2023-29013	Traefik (pronounced traffic) is a modern HTTP reverse proxy and load balancer for deploying microservices. There is a vulnerability in Go when parsing the HTTP headers, which impacts Traefik. HTTP header parsing could allocate substantially more memory than required to hold the parsed headers. This behavior could be exploited to cause a denial of service. This issue has been patched in versions 2.9.10 and 2.10.0-rc2.	7.5	More Details
CVE-2022-33270	Transient DOS due to time-of-check time-of-use race condition in Modem while processing RRC Reconfiguration message.	7.5	More Details
CVE-2022-33223	Transient DOS in Modem due to null pointer dereference while processing the incoming packet with http chunked encoding.	7.5	More Details
CVE-2022-25739	Denial of service in modem due to missing null check while processing the ipv6 packet received during ECM call	7.5	More Details
CVE-2022-25737	Information disclosure in modem due to missing NULL check while reading packets received from local network	7.5	More Details
CVE-2022-25731	Information disclosure in modem due to buffer over-read while processing packets from DNS server	7.5	More Details
CVE-2023-30515	Jenkins Thycotic DevOps Secrets Vault Plugin 1.0.0 and earlier does not properly mask (i.e., replace with asterisks) credentials in the build log when push mode for durable task logging is enabled.	7.5	More Details
CVE-2023-21930	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28974	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2.	7.4	More Details
CVE-2023-30535	Snowflake JDBC provides a JDBC type 4 driver that supports core functionality, allowing Java program to connect to Snowflake. Users of the Snowflake JDBC driver were vulnerable to a command injection vulnerability. An attacker could set up a malicious, publicly accessible server which responds to the SSO URL with an attack payload. If the attacker then tricked a user into visiting the maliciously crafted connection URL, the user's local machine would render the malicious payload, leading to a remote code execution. The vulnerability was patched on March 17, 2023 as part of Snowflake JDBC driver Version 3.13.29. All users should immediately upgrade the Snowflake JDBC driver to the latest version: 3.13.29.	7.3	More Details
CVE-2023-2073	A vulnerability was found in Campcodes Online Traffic Offense Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /classes/Login.php. The manipulation of the argument password leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-226051.	7.3	More Details
CVE-2023-30459	SmartPTT SCADA 1.1.0.0 allows remote code execution (when the attacker has administrator privileges) by writing a malicious C# script and executing it on the server (via server settings in the administrator control panel on port 8101, by default).	7.2	More Details
CVE-2023-29855	WBCE CMS 1.5.3 has a command execution vulnerability via admin/languages/install.php.	7.2	More Details
CVE-2023-21932	Vulnerability in the Oracle Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: OXI). The supported version that is affected is 5.6. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5 Property Services. While the vulnerability is in Oracle Hospitality OPERA 5 Property 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 Hospitality OPERA 5 Property Services accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality OPERA 5 Property Services accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:L/A:L).	7.2	More Details
CVE-2023-27733	DedeCMS v5.7.106 was discovered to contain a SQL injection vulnerability via the component /dede/sys_sql_query.php.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25550	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists that allows remote code execution via the “hostname” parameter when maliciously crafted hostname syntax is entered. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior)	7.2	More Details
CVE-2023-29410	A CWE-20: Improper Input Validation vulnerability exists that could allow an authenticated attacker to gain the same privilege as the application on the server when a malicious payload is provided over HTTP for the server to execute.	7.2	More Details
CVE-2023-1831	Mattermost fails to redact from audit logs the user password during user creation and the user password hash in other operations if the experimental audit logging configuration was enabled (ExperimentalAuditSettings section in config).	7.2	More Details
CVE-2023-25549	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists that allows for remote code execution when using a parameter of the DCE network settings endpoint. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior)	7.2	More Details
CVE-2023-0277	The WC Fields Factory WordPress plugin through 4.1.5 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin	7.2	More Details
CVE-2023-29084	Zoho ManageEngine ADManager Plus before 7181 allows for authenticated users to exploit command injection via Proxy settings.	7.2	More Details
CVE-2023-28971	An Improper Restriction of Communication Channel to Intended Endpoints vulnerability in the timescaledb feature of Juniper Networks Paragon Active Assurance (PAA) (Formerly Netrounds) allows an attacker to bypass existing firewall rules and limitations used to restrict internal communcations. The Test Agents (TA) Appliance connects to the Control Center (CC) using OpenVPN. TA's are assigned an internal IP address in the 100.70.0.0/16 range. Firewall rules exists to limit communication from TA's to the CC to specific services only. OpenVPN is configured to not allow direct communication between Test Agents in the OpenVPN application itself, and routing is normally not enabled on the server running the CC application. The timescaledb feature is installed as an optional package on the Control Center. When the timescaledb container is started, this causes side-effects by bypassing the existing firewall rules and limitations for Test Agent communications. Note: This issue only affects customers hosting their own on-prem Control Center. The Paragon Active Assurance Software as a Service (SaaS) is not affected by this vulnerability since the timescaledb service is not enabled. This issue affects all on-prem versions of Juniper Networks Paragon Active Assurance prior to 4.1.2.	7.2	More Details
CVE-2023-26852	An arbitrary file upload vulnerability in the upload plugin of Textpattern v4.8.8 and below allows attackers to execute arbitrary code by uploading a crafted PHP file.	7.2	More Details
CVE-2023-29002	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. When run in debug mode, Cilium will log the contents of the `cilium-secrets` namespace. This could include data such as TLS private keys for Ingress and GatewayAPI resources. An attacker with access to debug output from the Cilium containers could use the resulting output to intercept and modify traffic to and from the affected cluster. Output of the sensitive information would occur at Cilium agent restart, when secrets in the namespace are modified, and on creation of Ingress or GatewayAPI resources. This vulnerability is fixed in Cilium releases 1.11.16, 1.12.9, and 1.13.2. Users unable to upgrade should disable debug mode.	7.2	More Details
CVE-2023-30638	Atos Unify OpenScape SBC 10 before 10R3.1.3, OpenScape Branch 10 before 10R3.1.2, and OpenScape BCF 10 before 10R10.7.0 allow remote authenticated admins to inject commands.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27647	An issue found in DUALSPACE Lock Master v.2.2.4 allows a local attacker to cause a denial of service or gain sensitive information via the com.ludashi.superlock.util.pref.SharedPrefProviderEntryMethod: insert of the android.net.Uri.insert method.	7.1	More Details
CVE-2023-30630	Dmidecode before 3.5 allows -dump-bin to overwrite a local file. This has security relevance because, for example, execution of Dmidecode via Sudo is plausible.	7.1	More Details
CVE-2023-21980	Vulnerability in the MySQL Server product of Oracle MySQL (component: Client programs). Supported versions that are affected are 5.7.41 and prior and 8.0.32 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H).	7.1	More Details
CVE-2023-28973	An Improper Authorization vulnerability in the 'sysmanctl' shell command of Juniper Networks Junos OS Evolved allows a local, authenticated attacker to execute administrative commands that could impact the integrity of the system or system availability. Administrative functions such as daemon restarting, routing engine (RE) switchover, and node shutdown can all be performed through exploitation of the 'sysmanctl' command. Access to the 'sysmanctl' command is only available from the Junos shell. Neither direct nor indirect access to 'sysmanctl' is available from the Junos CLI. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S5-EVO; 21.2 versions prior to 21.2R3-EVO; 21.3 versions prior to 21.3R2-EVO; 21.4 versions prior to 21.4R1-S2-EVO, 21.4R2-EVO.	7.1	More Details
CVE-2023-30770	A stack-based buffer overflow vulnerability was found in the ASUSTOR Data Master (ADM) due to the lack of data size validation. An attacker can exploit this vulnerability to execute arbitrary code. Affected ADM versions include: 4.0.6.REG2, 4.1.0 and below as well as 4.2.0.RE71 and below.	7.1	More Details
CVE-2022-45836	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in W3 Eden, Inc. Download Manager plugin <= 3.2.59 versions.	7.1	More Details
CVE-2023-26980	PAX Technology PAX A920 Pro PayDroid 8.1suffers from a Race Condition vulnerability, which allows attackers to bypass the payment software and force the OS to boot directly to Android during the boot process. NOTE: the vendor disputes this because the attack is not feasible: the home launcher will be loaded before any user applications.	7.0	More Details
CVE-2023-21896	Vulnerability in the Oracle Solaris product of Oracle Systems (component: NSSwitch). Supported versions that are affected are 10 and 11. Difficult to exploit 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. CVSS 3.1 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	7.0	More Details
CVE-2023-21922	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Health Sciences InForm. 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 Health Sciences InForm accessible data as well as unauthorized access to critical data or complete access to all Oracle Health Sciences InForm accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N).	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29086	An issue was discovered in Samsung Exynos Mobile Processor, Automotive Processor and Modem for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos 9110, and Exynos Auto T5123. Memory corruption can occur due to insufficient parameter validation while decoding an SIP Min-SE header.	6.8	More Details
CVE-2023-29087	An issue was discovered in Samsung Exynos Mobile Processor, Automotive Processor and Modem for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos 9110, and Exynos Auto T5123. Memory corruption can occur due to insufficient parameter validation while decoding an SIP Retry-After header.	6.8	More Details
CVE-2023-29088	An issue was discovered in Samsung Exynos Mobile Processor, Automotive Processor and Modem for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos 9110, and Exynos Auto T5123. Memory corruption can occur due to insufficient parameter validation while decoding an SIP Session-Expires header.	6.8	More Details
CVE-2023-21934	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Difficult to exploit vulnerability allows low privileged attacker having User Account privilege with network access via TLS to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java VM accessible data as well as unauthorized access to critical data or complete access to all Java VM accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N).	6.8	More Details
CVE-2023-29089	An issue was discovered in Samsung Exynos Mobile Processor, Automotive Processor and Modem for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos 9110, and Exynos Auto T5123. Memory corruption can occur due to insufficient parameter validation while decoding SIP multipart messages.	6.8	More Details
CVE-2023-29090	An issue was discovered in Samsung Exynos Mobile Processor, Automotive Processor and Modem for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos 9110, and Exynos Auto T5123. Memory corruption can occur due to insufficient parameter validation while decoding an SIP Via header.	6.8	More Details
CVE-2023-29091	An issue was discovered in Samsung Exynos Mobile Processor, Automotive Processor and Modem for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos 9110, and Exynos Auto T5123. Memory corruption can occur due to insufficient parameter validation while decoding an SIP URI.	6.8	More Details
CVE-2022-33289	Memory corruption occurs in Modem due to improper validation of array index when malformed APDU is sent from card.	6.8	More Details
CVE-2022-33297	Information disclosure due to buffer overread in Linux sensors	6.8	More Details
CVE-2022-33302	Memory corruption due to improper validation of array index in User Identity Module when APN TLV length is greater than command length.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21918	Vulnerability in the Oracle Database Recovery Manager component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Easily exploitable vulnerability allows high privileged attacker having Local SYSDBA privilege with network access via Oracle Net to compromise Oracle Database Recovery Manager. While the vulnerability is in Oracle Database Recovery Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Database Recovery Manager. CVSS 3.1 Base Score 6.8 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H).	6.8	More Details
CVE-2023-29085	An issue was discovered in Samsung Exynos Mobile Processor, Automotive Processor and Modem for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos 9110, and Exynos Auto T5123. Memory corruption can occur due to insufficient parameter validation while decoding an SIP status line.	6.8	More Details
CVE-2023-28972	An Improper Link Resolution Before File Access vulnerability in console port access of Juniper Networks Junos OS on NFX Series allows an attacker to bypass console access controls. When "set system ports console insecure" is enabled, root login is disallowed for Junos OS as expected. However, the root password can be changed using "set system root-authentication plain-text-password" on NFX Series systems, leading to a possible administrative bypass with physical access to the console. Password recovery, changing the root password from a console, should not have been allowed from an insecure console. This is similar to the vulnerability described in CVE-2019-0035 but affects different platforms and in turn requires a different fix. This issue affects Juniper Networks Junos OS on NFX Series: 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-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2.	6.8	More Details
CVE-2023-30542	OpenZeppelin Contracts is a library for secure smart contract development. The proposal creation entrypoint (`propose`) in `GovernorCompatibilityBravo` allows the creation of proposals with a `signatures` array shorter than the `calldatas` array. This causes the additional elements of the latter to be ignored, and if the proposal succeeds the corresponding actions would eventually execute without any calldata. The `ProposalCreated` event correctly represents what will eventually execute, but the proposal parameters as queried through `getActions` appear to respect the original intended calldata. This issue has been patched in 4.8.3. As a workaround, ensure that all proposals that pass through governance have equal length `signatures` and `calldatas` parameters.	6.8	More Details
CVE-2023-28140	An Executable Hijacking condition exists in the Qualys Cloud Agent for Windows platform in versions before 4.5.3.1. Attackers may load a malicious copy of a Dependency Link Library (DLL) via a local attack vector instead of the DLL that the application was expecting, when processes are running with escalated privileges. This vulnerability is bounded only to the time of uninstallation and can only be exploited locally. At the time of this disclosure, versions before 4.0 are classified as End of Life.	6.7	More Details
CVE-2022-33298	Memory corruption due to use after free in Modem while modem initialization.	6.7	More Details
CVE-2023-28142	A Race Condition exists in the Qualys Cloud Agent for Windows platform in versions from 3.1.3.34 and before 4.5.3.1. This allows attackers to escalate privileges limited on the local machine during uninstallation of the Qualys Cloud Agent for Windows. Attackers may gain SYSTEM level privileges on that asset to run arbitrary commands. At the time of this disclosure, versions before 4.0 are classified as End of Life.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28141	An NTFS Junction condition exists in the Qualys Cloud Agent for Windows platform in versions before 4.8.0.31. Attackers may write files to arbitrary locations via a local attack vector. This allows attackers to assume the privileges of the process, and they may delete or otherwise on unauthorized files, allowing for the potential modification or deletion of sensitive files limited only to that specific directory/file object. This vulnerability is bounded to the time of installation/uninstallation and can only be exploited locally. At the time of this disclosure, versions before 4.0 are classified as End of Life.	6.7	More Details
CVE-2023-28143	Qualys Cloud Agent for macOS (versions 2.5.1-75 before 3.7) installer allows a local escalation of privilege bounded only to the time of installation and only on older macOSX (macOS 10.15 and older) versions. Attackers may exploit incorrect file permissions to give them ROOT command execution privileges on the host. During the install of the PKG, a step in the process involves extracting the package and copying files to several directories. Attackers may gain writable access to files during the install of PKG when extraction of the package and copying files to several directories, enabling a local escalation of privilege.	6.7	More Details
CVE-2023-28003	A CWE-613: Insufficient Session Expiration vulnerability exists that could allow an attacker to maintain unauthorized access over a hijacked session in PME after the legitimate user has signed out of their account.	6.7	More Details
CVE-2022-33301	Memory corruption due to incorrect type conversion or cast in audio while using audio playback/capture when crafted address is sent from AGM IPC to AGM.	6.7	More Details
CVE-2022-37705	A privilege escalation flaw was found in Amanda 3.5.1 in which the backup user can acquire root privileges. The vulnerable component is the runtar SUID program, which is a wrapper to run /usr/bin/tar with specific arguments that are controllable by the attacker. This program mishandles the arguments passed to tar binary (it expects that the argument name and value are separated with a space; however, separating them with an equals sign is also supported),	6.7	More Details
CVE-2022-37704	Amanda 3.5.1 allows privilege escalation from the regular user backup to root. The SUID binary located at /lib/amanda/rundump will execute /usr/sbin/dump as root with controlled arguments from the attacker which may lead to escalation of privileges, denial of service, and information disclosure.	6.7	More Details
CVE-2023-21969	Vulnerability in Oracle SQL Developer (component: Installation). Supported versions that are affected are Prior to 23.1.0. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle SQL Developer executes to compromise Oracle SQL Developer. Successful attacks of this vulnerability can result in takeover of Oracle SQL Developer. CVSS 3.1 Base Score 6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	6.7	More Details
CVE-2023-28965	An Improper Check or Handling of Exceptional Conditions within the storm control feature of Juniper Networks Junos OS allows an attacker sending a high rate of traffic to cause a Denial of Service. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. Storm control monitors the level of applicable incoming traffic and compares it with the level specified. If the combined level of the applicable traffic exceeds the specified level, the switch drops packets for the controlled traffic types. This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-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; 21.4 versions prior to 21.4R2.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28981	An Improper Input Validation vulnerability in the kernel of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). If the receipt of router advertisements is enabled on an interface and a specifically malformed RA packet is received, memory corruption will happen which leads to an rpd crash. This issue affects: Juniper Networks Junos OS 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2; 22.1 versions prior to 22.1R2. Juniper Networks Junos OS Evolved 20.3-EVO version 20.3R1-EVO and later versions; 20.4-EVO versions prior to 20.4R3-S6-EVO; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO.	6.5	More Details
CVE-2023-0004	A local file deletion vulnerability in Palo Alto Networks PAN-OS software enables an authenticated administrator to delete files from the local file system with elevated privileges. These files can include logs and system components that impact the integrity and availability of PAN-OS software.	6.5	More Details
CVE-2023-28488	client.c in gdhcp in ConnMan through 1.41 could be used by network-adjacent attackers (operating a crafted DHCP server) to cause a stack-based buffer overflow and denial of service, terminating the connman process.	6.5	More Details
CVE-2023-30516	Jenkins Image Tag Parameter Plugin 2.0 improperly introduces an option to opt out of SSL/TLS certificate validation when connecting to Docker registries, resulting in job configurations using Image Tag Parameters that were created before 2.0 having SSL/TLS certificate validation disabled by default.	6.5	More Details
CVE-2023-30532	A missing permission check in Jenkins TurboScript Plugin 1.3 and earlier allows attackers with Item/Read permission to trigger builds of jobs corresponding to the attacker-specified repository.	6.5	More Details
CVE-2023-24513	On affected platforms running Arista CloudEOS an issue in the Software Forwarding Engine (Sfe) can lead to a potential denial of service attack by sending malformed packets to the switch. This causes a leak of packet buffers and if enough malformed packets are received, the switch may eventually stop forwarding traffic.	6.5	More Details
CVE-2020-27545	libdwarf before 20201017 has a one-byte out-of-bounds read because of an invalid pointer dereference via an invalid line table in a crafted object.	6.5	More Details
CVE-2023-30531	Jenkins Consul KV Builder Plugin 2.0.13 and earlier does not mask the HashiCorp Consul ACL Token on the global configuration form, increasing the potential for attackers to observe and capture it.	6.5	More Details
CVE-2019-14944	An issue was discovered in GitLab Community and Enterprise Edition before 11.11.8, 12 before 12.0.6, and 12.1 before 12.1.6. Gitaly allows injection of command-line flags. This sometimes leads to privilege escalation or remote code execution.	6.5	More Details
CVE-2023-21910	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Web General). Supported versions that are affected are 6.4.0.0.0 and 12.2.1.4.0. 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 access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition 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 Number	Description	Base Score	Reference
CVE-2023-28970	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing on the network interfaces of Juniper Networks Junos OS on JRR200 route reflector appliances allows an adjacent, network-based attacker sending a specific packet to the device to cause a kernel 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 can only be triggered by an attacker on the local broadcast domain. Packets routed to the device are unable to trigger this crash. This issue affects Juniper Networks Junos OS on JRR200: All 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 22.2R2-S2, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; 22.4 versions prior to 22.4R1-S1, 22.4R2.	6.5	More Details
CVE-2022-43378	A CWE-1021: Improper Restriction of Rendered UI Layers or Frames vulnerability exists that could cause the user to be tricked into performing unintended actions when external address frames are not properly restricted. Affected Products: NetBotz 4 - 355/450/455/550/570 (V4.7.0 and prior)	6.5	More Details
CVE-2023-21909	Vulnerability in the Siebel CRM product of Oracle Siebel CRM (component: UI Framework). Supported versions that are affected are 23.3 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel CRM. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel CRM 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-2023-30528	Jenkins WSO2 Oauth Plugin 1.0 and earlier does not mask the WSO2 Oauth client secret on the global configuration form, increasing the potential for attackers to observe and capture it.	6.5	More Details
CVE-2023-30526	A missing permission check in Jenkins Report Portal Plugin 0.5 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified bearer token authentication.	6.5	More Details
CVE-2023-30512	CubeFS through 3.2.1 allows Kubernetes cluster-level privilege escalation. This occurs because DaemonSet has cfs-csi-cluster-role and can thus list all secrets, including the admin secret.	6.5	More Details
CVE-2023-21993	Vulnerability in the Oracle Clinical Remote Data Capture product of Oracle Health Sciences Applications (component: Forms). The supported version that is affected is 5.4.0.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Clinical Remote Data Capture. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Clinical Remote Data Capture 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-2020-28163	libdwarf before 20201201 allows a dwarf_print_lines.c NULL pointer dereference and application crash via a DWARF5 line-table header that has an invalid FORM for a pathname.	6.5	More Details
CVE-2022-34125	front/icon.send.php in the CMDB plugin before 3.0.3 for GLPI allows attackers to gain read access to sensitive information via a _log/ pathname in the file parameter.	6.5	More Details
CVE-2023-0889	Themeflection Numbers WordPress plugin before 2.0.1 does not have authorisation and CSRF check in an AJAX action, and does not ensure that the options to be updated belong to the plugin. As a result, it could allow any authenticated users, such as subscriber, to update arbitrary blog options, such as enabling registration and set the default role to administrator	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1274	The Pricing Tables For WPBakery Page Builder (formerly Visual Composer) WordPress plugin before 3.0 does not validate some shortcode attributes before using them to generate paths passed to include function/s, allowing any authenticated users such as subscriber to perform LFI attacks	6.5	More Details
CVE-2023-21978	Vulnerability in the Oracle Application Object Library product of Oracle E-Business Suite (component: GUI). Supported versions that are affected are 12.2.3-12.2.11. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Application Object Library. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Object Library, 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 Application Object Library accessible data as well as unauthorized read access to a subset of Oracle Application Object Library accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Application Object Library. 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-2022-48314	The Bluetooth module has a vulnerability of bypassing the user confirmation in the pairing process. Successful exploitation of this vulnerability may affect confidentiality.	6.5	More Details
CVE-2023-30539	Nextcloud is a personal home server system. Depending on the set up tags and other workflows this issue can be used to limit access of others or being able to grant them access when there are system tag based files access control or files retention rules. It is recommended that the Nextcloud Server is upgraded to 24.0.11 or 25.0.5, the Nextcloud Enterprise Server to 21.0.9.11, 22.2.10.11, 23.0.12.6, 24.0.11 or 25.0.5, and the Nextcloud Files automated tagging app to 1.11.1, 1.12.1, 1.13.1, 1.14.2, 1.15.3 or 1.16.1. Users unable to upgrade should disable all workflow related apps. Users are advised to upgrade.	6.5	More Details
CVE-2022-48313	The Bluetooth module has a vulnerability of bypassing the user confirmation in the pairing process. Successful exploitation of this vulnerability may affect confidentiality.	6.5	More Details
CVE-2022-45170	An issue was discovered in LIVEBOX Collaboration vDesk through v018. A Cryptographic Issue can occur under the /api/v1/vencrypt/decrypt/file endpoint. A malicious user, logged into a victim's account, is able to decipher a file without knowing the key set by the user.	6.5	More Details
CVE-2022-45175	An issue was discovered in LIVEBOX Collaboration vDesk through v018. An Insecure Direct Object Reference can occur under the 5.6.5-3/doc/{ID-FILE]/c/{N]/{C]/websocket endpoint. A malicious unauthenticated user can access cached files in the OnlyOffice backend of other users by guessing the file ID of a target file.	6.5	More Details
CVE-2023-1331	The Redirection WordPress plugin before 1.1.5 does not have CSRF checks in the uninstall action, which could allow attackers to make logged in admins delete all the redirections through a CSRF attack.	6.5	More Details
CVE-2022-45180	An issue was discovered in LIVEBOX Collaboration vDesk through v018. Broken Access Control exists under the /api/v1/vdesk_{DOMAIN]/export endpoint. A malicious user, authenticated to the product without any specific privilege, can use the API for exporting information about all users of the system (an operation intended to only be available to the system administrator).	6.5	More Details
CVE-2023-20866	In Spring Session version 3.0.0, the session id can be logged to the standard output stream. This vulnerability exposes sensitive information to those who have access to the application logs and can be used for session hijacking. Specifically, an application is vulnerable if it is using HeaderHttpSessionIdResolver.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20863	In spring framework versions prior to 5.2.24 release+ ,5.3.27+ and 6.0.8+ , it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.	6.5	More Details
CVE-2023-1371	The W4 Post List WordPress plugin before 2.4.6 does not ensure that password protected posts can be accessed before displaying their content, which could allow any authenticated users to access them	6.5	More Details
CVE-2023-21984	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Libraries). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2023-22897	An issue was discovered in SecurePoint UTM before 12.2.5.1. The firewall's endpoint at /spcgi.cgi allows information disclosure of memory contents to be achieved by an authenticated user. Essentially, uninitialized data can be retrieved via an approach in which a sessionid is obtained but not used.	6.5	More Details
CVE-2023-28959	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing of Juniper Networks Junos OS on QFX10002 allows an unauthenticated, adjacent attacker on the local broadcast domain sending a malformed packet to the device, causing all PFEs other than the inbound PFE to wedge and to eventually restart, resulting in a Denial of Service (DoS) condition. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue can only be triggered by sending a specific malformed packet to the device. Transit traffic does not trigger this issue. An indication of this issue occurring can be seen through the following log messages: fpc0 expr_hostbound_packet_handler: Receive pe 73? fpc0 Cmerror Op Set: PE Chip: PE0[0]: PGQ:misc_intr: 0x00000020: Enqueue of a packet with out-of-range VOQ in 192K-VOQ mode (URI: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL) The logs list below can also be observed when this issue occurs fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107), scope: pfe, category: functional, severity: major, module: PE Chip, type: Description for PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107) in module: PE Chip with scope: pfe category: functional level: major fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a), scope: pfe, category: functional, severity: fatal, module: PE Chip, type: Description for PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal fpc0 Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.1R3-S10; 19.4 versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1697	An Improper Handling of Missing Values vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause a dcpfe process core and thereby a Denial of Service (DoS). Continued receipt of these specific frames will cause a sustained Denial of Service condition. This issue occurs when a specific malformed ethernet frame is received. This issue affects Juniper Networks Junos OS on QFX10000 Series, PTX1000 Series Series: All versions prior to 19.4R3-S10; 20.1 version 20.1R1 and later versions; 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-S3; 21.4 versions prior to 21.4R3-S1; 22.1 versions prior to 22.1R2-S1, 22.1R3; 22.2 versions prior to 22.2R1-S2, 22.2R2.	6.5	More Details
CVE-2023-21946	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 and prior. Easily exploitable 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. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2023-29004	hap-wi/roxy-wi is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. A Path Traversal vulnerability was found in the current version of Roxy-WI (6.3.9.0 at the moment of writing this report). The vulnerability can be exploited via an HTTP request to /app/options.py and the config_file_name parameter. Successful exploitation of this vulnerability could allow an attacker with user level privileges to obtain the content of arbitrary files on the file server within the scope of what the server process has access to. The root-cause of the vulnerability lies in the get_config function of the /app/modules/config/config.py file, which only checks for relative path traversal, but still allows to read files from absolute locations passed via the config_file_name parameter.	6.5	More Details
CVE-2023-30536	slim/psr7 is a PSR-7 implementation for use with Slim 4. In versions prior to 1.6.1 an attacker could sneak in a newline (\n) into both the header names and values. While the specification states that \r\n\r\n is used to terminate the header list, many servers in the wild will also accept \n\n. An attacker that is able to control the header names that are passed to Slilm-Psr7 would be able to intentionally craft invalid messages, possibly causing application errors or invalid HTTP requests being sent out with an PSR-18 HTTP client. The latter might present a denial of service vector if a remote service's web application firewall bans the application due to the receipt of malformed requests. The issue has been patched in version 1.6.1. There are no known workarounds to this issue. Users are advised to upgrade.	6.5	More Details
CVE-2023-20118	A vulnerability in the web-based management interface of Cisco Small Business Routers RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary commands on an affected device. This vulnerability is due to improper validation of user input within incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface. A successful exploit could allow the attacker to gain root-level privileges and access unauthorized data. To exploit this vulnerability, an attacker would need to have valid administrative credentials on the affected device. Cisco has not and will not release software updates that address this vulnerability.	6.5	More Details
CVE-2023-22950	An issue was discovered in TigerGraph Enterprise Free Edition 3.x. Data loading jobs in gsql_server, created by any user with designer permissions, can read sensitive data from arbitrary locations.	6.5	More Details
CVE-2023-30772	The Linux kernel before 6.2.9 has a race condition and resultant use-after-free in drivers/power/supply/da9150-charger.c if a physically proximate attacker unplugs a device.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22946	In Apache Spark versions prior to 3.4.0, applications using spark-submit can specify a 'proxy-user' to run as, limiting privileges. The application can execute code with the privileges of the submitting user, however, by providing malicious configuration-related classes on the classpath. This affects architectures relying on proxy-user, for example those using Apache Livy to manage submitted applications. Update to Apache Spark 3.4.0 or later, and ensure that spark.submit.proxyUser.allowCustomClasspathInClusterMode is set to its default of "false", and is not overridden by submitted applications.	6.4	More Details
CVE-2023-2148	A vulnerability classified as critical has been found in Campcodes Online Thesis Archiving System 1.0. This affects an unknown part of the file /admin/curriculum/view_curriculum.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-226269 was assigned to this vulnerability.	6.3	More Details
CVE-2023-2144	A vulnerability was found in Campcodes Online Thesis Archiving System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/departments/view_department.php. The manipulation of the argument id 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-226265 was assigned to this vulnerability.	6.3	More Details
CVE-2023-2160	Weak Password Requirements in GitHub repository modoboa/modoboa prior to 2.1.0.	6.3	More Details
CVE-2022-34755	A CWE-427 - Uncontrolled Search Path Element vulnerability exists that could allow an attacker with a local privileged account to place a specially crafted file on the target machine, which may give the attacker the ability to execute arbitrary code during the installation process initiated by a valid user. Affected Products: Easergy Builder Installer (1.7.23 and prior)	6.3	More Details
CVE-2023-2151	A vulnerability, which was classified as critical, was found in SourceCodester Student Study Center Desk Management System 1.0. Affected is an unknown function of the file manage_student.php. The manipulation of the argument id 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-226272.	6.3	More Details
CVE-2021-34337	An issue was discovered in Mailman Core before 3.3.5. An attacker with access to the REST API could use timing attacks to determine the value of the configured REST API password and then make arbitrary REST API calls. The REST API is bound to localhost by default, limiting the ability for attackers to exploit this, but can optionally be made to listen on other interfaces.	6.3	More Details
CVE-2023-2147	A vulnerability was found in Campcodes Online Thesis Archiving System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/students/view_details.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-226268.	6.3	More Details
CVE-2015-10102	A vulnerability, which was classified as critical, has been found in Freshdesk Plugin 1.7 on WordPress. Affected by this issue is some unknown functionality. The manipulation leads to open redirect. The attack may be launched remotely. Upgrading to version 1.8 is able to address this issue. The patch is identified as 2aaecd4e0c7c6c1dc4e6a593163d5f7aa0fa5d5b. It is recommended to upgrade the affected component. VDB-226118 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2108	A vulnerability has been found in SourceCodester Judging Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file edit_contestant.php. The manipulation of the argument contestant_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-226147.	6.3	More Details
CVE-2023-2145	A vulnerability was found in Campcodes Online Thesis Archiving System 1.0. It has been classified as critical. Affected is an unknown function of the file projects_per_curriculum.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-226266 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-2149	A vulnerability classified as critical was found in Campcodes Online Thesis Archiving System 1.0. This vulnerability affects unknown code of the file /admin/user/manage_user.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-226270 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-2146	A vulnerability was found in Campcodes Online Thesis Archiving System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file classes/Master.php. The manipulation of the argument name leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-226267.	6.3	More Details
CVE-2023-2130	A vulnerability classified as critical has been found in SourceCodester Purchase Order Management System 1.0. Affected is an unknown function of the file /admin/suppliers/view_details.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-226206 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-2053	A vulnerability, which was classified as critical, has been found in Campcodes Advanced Online Voting System 1.0. Affected by this issue is some unknown functionality of the file /admin/candidates_row.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-225938 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-1993	LISP dissector large loop in Wireshark 4.0.0 to 4.0.4 and 3.6.0 to 3.6.12 allows denial of service via packet injection or crafted capture file	6.3	More Details
CVE-2023-1992	RPCoRDMA dissector crash in Wireshark 4.0.0 to 4.0.4 and 3.6.0 to 3.6.12 allows denial of service via packet injection or crafted capture file	6.3	More Details
CVE-2023-2074	A vulnerability was found in Campcodes Online Traffic Offense Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /classes/Master.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-226052.	6.3	More Details
CVE-2023-2038	A vulnerability was found in Campcodes Video Sharing Website 1.0. It has been declared as critical. This vulnerability affects unknown code of the file admin_class.php. The manipulation of the argument email 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-225916.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2056	A vulnerability was found in DedeCMS up to 5.7.87 and classified as critical. This issue affects the function GetSystemFile of the file module_main.php. The manipulation leads to code injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-225941 was assigned to this vulnerability.	6.3	More Details
CVE-2023-2035	A vulnerability has been found in Campcodes Video Sharing Website 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file signup.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-225913 was assigned to this vulnerability.	6.3	More Details
CVE-2023-2036	A vulnerability was found in Campcodes Video Sharing Website 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file upload.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-225914 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-2054	A vulnerability, which was classified as critical, was found in Campcodes Advanced Online Voting System 1.0. This affects an unknown part of the file /admin/positions_delete.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-225939.	6.3	More Details
CVE-2023-2052	A vulnerability classified as critical was found in Campcodes Advanced Online Voting System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/ballot_down.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-225937 was assigned to this vulnerability.	6.3	More Details
CVE-2023-2051	A vulnerability classified as critical has been found in Campcodes Advanced Online Voting System 1.0. Affected is an unknown function of the file /admin/positions_row.php. The manipulation of the argument id 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-225936.	6.3	More Details
CVE-2023-2050	A vulnerability was found in Campcodes Advanced Online Voting System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/positions_add.php. The manipulation of the argument description leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-225935.	6.3	More Details
CVE-2023-1994	GQUIC dissector crash in Wireshark 4.0.0 to 4.0.4 and 3.6.0 to 3.6.12 allows denial of service via packet injection or crafted capture file	6.3	More Details
CVE-2023-2049	A vulnerability was found in Campcodes Advanced Online Voting System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/ballot_up.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-225934 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-0006	A local file deletion vulnerability in the Palo Alto Networks GlobalProtect app on Windows devices enables a user to delete system files from the endpoint with elevated privileges through a race condition.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2048	A vulnerability was found in Campcodes Advanced Online Voting System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/voters_row.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-225933 was assigned to this vulnerability.	6.3	More Details
CVE-2023-2047	A vulnerability was found in Campcodes Advanced Online Voting System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file login.php. The manipulation of the argument voter leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-225932.	6.3	More Details
CVE-2023-2037	A vulnerability was found in Campcodes Video Sharing Website 1.0. It has been classified as critical. This affects an unknown part of the file watch.php. The manipulation of the argument code leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-225915.	6.3	More Details
CVE-2023-2043	A vulnerability, which was classified as problematic, was found in Control iD RHiD 23.3.19.0. This affects an unknown part of the file /v2/customerdb/operator.svc/a of the component Edit Handler. The manipulation of the argument email leads to sql injection. It is possible to initiate the attack remotely. The identifier VDB-225921 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-2023-2042	A vulnerability, which was classified as problematic, has been found in DataGear up to 4.7.0/5.1.0. Affected by this issue is some unknown functionality of the component JDBC Server Handler. The manipulation leads to deserialization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-2041	A vulnerability classified as critical was found in novel-plus 3.6.2. Affected by this vulnerability is an unknown functionality of the file /category/list?limit=10&offset=0&order=desc. The manipulation of the argument sort leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-225919. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-2040	A vulnerability classified as critical has been found in novel-plus 3.6.2. Affected is an unknown function of the file /news/list?limit=10&offset=0&order=desc. The manipulation of the argument sort leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-225918 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-2023-2075	A vulnerability classified as critical has been found in Campcodes Online Traffic Offense Management System 1.0. This affects an unknown part of the file /admin/offenses/view_details.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-226053 was assigned to this vulnerability.	6.3	More Details
CVE-2023-2039	A vulnerability was found in novel-plus 3.6.2. It has been rated as critical. This issue affects some unknown processing of the file /author/list?limit=10&offset=0&order=desc. The manipulation of the argument sort 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-225917 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 Number	Description	Base Score	Reference
CVE-2023-2095	A vulnerability was found in SourceCodester Vehicle Service Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/maintenance/manage_category.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-226103.	6.3	More Details
CVE-2023-2094	A vulnerability has been found in SourceCodester Vehicle Service Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/mechanics/manage_mechanic.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-226102 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-2107	A vulnerability, which was classified as critical, was found in IBOS 4.5.5. Affected is an unknown function of the file file/personal/del&op=recycle. The manipulation of the argument fids leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-226110 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-2089	A vulnerability was found in SourceCodester Complaint Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/userprofile.php of the component GET Parameter Handler. The manipulation of the argument uid 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-226097 was assigned to this vulnerability.	6.3	More Details
CVE-2023-2090	A vulnerability classified as critical has been found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0. Affected is an unknown function of the file /admin/maintenance/view_designation.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-226098 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-2097	A vulnerability was found in SourceCodester Vehicle Service Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /classes/Master.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-226105 was assigned to this vulnerability.	6.3	More Details
CVE-2023-2092	A vulnerability, which was classified as critical, has been found in SourceCodester Vehicle Service Management System 1.0. Affected by this issue is some unknown functionality of the file view_service.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-226100.	6.3	More Details
CVE-2023-2096	A vulnerability was found in SourceCodester Vehicle Service Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/service_requests/manage_inventory.php. The manipulation of the argument id 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-226104.	6.3	More Details
CVE-2023-2093	A vulnerability, which was classified as critical, was found in SourceCodester Vehicle Service Management System 1.0. This affects an unknown part of the file /classes/Login.php. The manipulation of the argument username leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-226101 was assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24934	Microsoft Defender Security Feature Bypass Vulnerability	6.2	More Details
CVE-2023-1413	The WP VR WordPress plugin before 8.2.9 does not sanitise and escape some parameters before outputting them 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-2023-21905	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: Routing Hub). Supported versions that are affected are 14.5, 14.6 and 14.7. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. 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 Banking Virtual Account Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Banking Virtual Account Management accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N).	6.1	More Details
CVE-2023-27666	Auto Dealer Management System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the name parameter at /classes/SystemSettings.php?f=update_settings.	6.1	More Details
CVE-2023-2109	Cross-site Scripting (XSS) - DOM in GitHub repository chatwoot/chatwoot prior to 2.14.0.	6.1	More Details
CVE-2023-21906	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: SMS Module). Supported versions that are affected are 14.5, 14.6 and 14.7. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. 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 Banking Virtual Account Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Banking Virtual Account Management accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N).	6.1	More Details
CVE-2023-2119	The Responsive Filterable Portfolio plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the search_term parameter in versions up to, and including, 1.0.19 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-2023-27092	Cross Site Scripting vulnerability found in Jbootfly allows attackers to obtain sensitive information via the username parameter.	6.1	More Details
CVE-2022-43697	OX App Suite before 7.10.6-rev30 allows XSS via an activity tracking adapter defined by jslob.	6.1	More Details
CVE-2023-29854	DirCMS 6.0.0 has a Cross Site Scripting (XSS) vulnerability in the foreground.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43696	OX App Suite before 7.10.6-rev20 allows XSS via upsell ads.	6.1	More Details
CVE-2023-2120	The Thumbnail carousel slider plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the search_term parameter in versions up to, and including, 1.1.9 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-2023-27572	An issue was discovered in CommScope Arris DG3450 Cable Gateway AR01.02.056.18_041520_711.NCS.10. A reflected XSS vulnerability was discovered in the https_redirect.php web page via the page parameter.	6.1	More Details
CVE-2023-1473	The Slider, Gallery, and Carousel by MetaSlider WordPress plugin 3.29.0 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-2023-1373	The W4 Post List WordPress plugin before 2.4.6 does not escape some URLs before outputting them in attributes, leading to Reflected Cross-Site Scripting	6.1	More Details
CVE-2018-17883	An issue was discovered in Open Ticket Request System (OTRS) 6.0.x before 6.0.12. An attacker could send an e-mail message with a malicious link to an OTRS system or an agent. If a logged-in agent opens this link, it could cause the execution of JavaScript in the context of OTRS.	6.1	More Details
CVE-2022-37306	OX App Suite before 7.10.6-rev30 allows XSS via an upsell trigger.	6.1	More Details
CVE-2022-46389	There exists a reflected XSS within the logout functionality of ServiceNow versions lower than Quebec Patch 10 Hotfix 11b, Rome Patch 10 Hotfix 3b, San Diego Patch 9, Tokyo Patch 4, and Utah GA. This enables an unauthenticated remote attacker to execute arbitrary JavaScript code in the browser-based web console.	6.1	More Details
CVE-2023-25551	A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists on a DCE file upload endpoint when tampering with parameters over HTTP. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior)	6.1	More Details
CVE-2023-25553	A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists on a DCE endpoint through the logging capabilities of the webserver. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior)	6.1	More Details
CVE-2023-1282	The Drag and Drop Multiple File Upload PRO - Contact Form 7 Standard WordPress plugin before 2.11.1 and Drag and Drop Multiple File Upload PRO - Contact Form 7 with Remote Storage Integrations WordPress plugin before 5.0.6.4 do 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 admins.	6.1	More Details
CVE-2022-28353	In the External Redirect Warning Plugin 1.3 for MyBB, the redirect URL (aka external.php?url=) is vulnerable to XSS.	6.1	More Details
CVE-2023-29623	Purchase Order Management v1.0 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the password parameter at /purchase_order/classes/login.php.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21956	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, 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 WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server 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-2023-26123	Versions of the package raysan5/raylib before 4.5.0 are vulnerable to Cross-site Scripting (XSS) such that the SetClipboardText API does not properly escape the ' character, allowing attacker-controlled input to break out of the string and execute arbitrary JavaScript via emscripten_run_script function. **Note:** This vulnerability is present only when compiling raylib for PLATFORM_WEB. All the other Desktop/Mobile/Embedded platforms are not affected.	6.1	More Details
CVE-2022-45838	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in Repute InfoSystems ARForms Form Builder plugin <= 1.5.5 versions.	6.1	More Details
CVE-2023-21989	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, 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 VM VirtualBox 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-2023-21907	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: OBVAM Trn Journal Domain). Supported versions that are affected are 14.5, 14.6 and 14.7. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Virtual Account Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Virtual Account Management accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Banking Virtual Account Management. CVSS 3.1 Base Score 6.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:H).	6.0	More Details
CVE-2023-21908	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: OBVAM Trn Journal Domain). Supported versions that are affected are 14.5, 14.6 and 14.7. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Virtual Account Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Virtual Account Management accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Banking Virtual Account Management. CVSS 3.1 Base Score 6.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:H).	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22002	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, 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 VM VirtualBox 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-2022-37186	In LemonLDAP::NG before 2.0.15. some sessions are not deleted when they are supposed to be deleted according to the timeoutActivity setting. This can occur when there are at least two servers, and a session is manually removed before the time at which it would have been removed automatically.	5.9	More Details
CVE-2023-25597	A vulnerability in the web conferencing component of Mitel MiCollab through 9.6.2.9 could allow an unauthenticated attacker to download a shared file via a crafted request - including the exact path and filename - due to improper authentication control. A successful exploit could allow access to sensitive information.	5.9	More Details
CVE-2023-21924	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Health Sciences InForm. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Health Sciences InForm, 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 Health Sciences InForm accessible data as well as unauthorized read access to a subset of Oracle Health Sciences InForm accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Health Sciences InForm. CVSS 3.1 Base Score 5.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L).	5.9	More Details
CVE-2022-33296	Memory corruption due to integer overflow to buffer overflow in Modem while parsing Traffic Channel Neighbor List Update message.	5.9	More Details
CVE-2019-14942	An issue was discovered in GitLab Community and Enterprise Edition before 11.11.8, 12 before 12.0.6, and 12.1 before 12.1.6. Cookies for GitLab Pages (which have access control) could be sent over cleartext HTTP.	5.9	More Details
CVE-2023-21967	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21954	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. 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 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	5.9	More Details
CVE-2023-28961	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah' from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance : Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2.	5.8	More Details
CVE-2023-21952	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). 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. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N).	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21986	Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Native Image). Supported versions that are affected are Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle GraalVM Enterprise Edition executes to compromise Oracle GraalVM Enterprise Edition. While the vulnerability is in Oracle GraalVM 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 GraalVM Enterprise Edition accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle GraalVM Enterprise Edition. CVSS 3.1 Base Score 5.7 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:L).	5.7	More Details
CVE-2023-21965	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). 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. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N).	5.7	More Details
CVE-2023-21970	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Security). 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 BI Publisher. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data. CVSS 3.1 Base Score 5.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N).	5.7	More Details
CVE-2023-25555	A CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability exists that could allow a user that knows the credentials to execute unprivileged shell commands on the appliance over SSH. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior)	5.6	More Details
CVE-2023-21960	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic Server. 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-2023-26382	Adobe Dimension version 3.4.8 (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 file.	5.5	More Details
CVE-2023-26380	Adobe Dimension version 3.4.8 (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 file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26381	Adobe Dimension version 3.4.8 (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 file.	5.5	More Details
CVE-2023-26379	Adobe Dimension version 3.4.8 (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 file.	5.5	More Details
CVE-2023-26378	Adobe Dimension version 3.4.8 (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 file.	5.5	More Details
CVE-2023-28856	Redis is an open source, in-memory database that persists on disk. Authenticated users can use the `HINCRBYFLOAT` command to create an invalid hash field that will crash Redis on access in affected versions. This issue has been addressed in in versions 7.0.11, 6.2.12, and 6.0.19. Users are advised to upgrade. There are no known workarounds for this issue.	5.5	More Details
CVE-2023-26377	Adobe Dimension version 3.4.8 (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 file.	5.5	More Details
CVE-2023-26376	Adobe Dimension version 3.4.8 (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 file.	5.5	More Details
CVE-2023-26375	Adobe Dimension version 3.4.8 (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 file.	5.5	More Details
CVE-2023-26374	Adobe Dimension version 3.4.8 (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 file.	5.5	More Details
CVE-2023-26401	Adobe Dimension version 3.4.8 (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 file.	5.5	More Details
CVE-2023-29581	yasm 1.3.0.55.g101bc has a segmentation violation in the function delete_Token at modules/preprocs/nasm/nasm-pp.c. NOTE: although a libyasm application could become unavailable if this were exploited, the vendor's position is that there is no security relevance because there is either supposed to be input validation before data reaches libyasm, or a sandbox in which the application runs.	5.5	More Details
CVE-2023-29571	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via gc_sweep at src/mjs_gc.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27704	Void Tools Everything lower than v1.4.1.1022 was discovered to contain a Regular Expression Denial of Service (ReDoS).	5.5	More Details
CVE-2023-29580	yasm 1.3.0.55.g101bc was discovered to contain a segmentation violation via the component yasm_expr_create at /libyasm/expr.c.	5.5	More Details
CVE-2023-28980	A Use After Free vulnerability in the routing protocol daemon of Juniper Networks Junos OS and Junos OS Evolved allows a locally authenticated attacker with low privileges to cause Denial of Service (DoS). In a rib sharding scenario the rpd process will crash shortly after specific CLI command is issued. This issue is more likely to occur in a scenario with high route scale (>1M routes). This issue affects: Juniper Networks Junos OS * 20.2 version 20.2R3-S5 and later versions prior to 20.2R3-S6; * 20.3 version 20.3R3-S2 and later versions prior to 20.3R3-S5; * 20.4 version 20.4R3-S1 and later versions prior to 20.4R3-S4 * 21.1 version 21.1R3 and later versions prior to 21.1R3-S3; * 21.2 version 21.2R1-S2, 21.2R2-S1 and later versions prior to 21.2R3-S2; * 21.3 version 21.3R2 and later versions prior to 21.3R3; * 21.4 versions prior to 21.4R2-S1, 21.4R3; * 22.1 versions prior to 22.1R2. Juniper Networks Junos OS Evolved * 20.4-EVO version 20.4R3-S1-EVO and later versions prior to 20.4R3-S6-EVO; * 21.2-EVO version 21.2R1-S2-EVO and later versions prior to 21.2R3-S4-EVO; * 21.3-EVO version 21.3R2-EVO and later versions prior to 21.3R3-S1-EVO; * 21.4-EVO versions prior to 21.4R2-S1-EVO, 21.4R3-EVO; * 22.1-EVO versions prior to 22.1R2-EVO.	5.5	More Details
CVE-2023-29574	Bento4 v1.6.0-639 was discovered to contain an out-of-memory bug in the mp42avc component.	5.5	More Details
CVE-2022-24350	An issue was discovered in IhisiSmm in Insyde InsydeH2O with kernel 5.0 through 5.5. IHISI function 0x17 verifies that the output buffer lies within the command buffer but does not verify that output data does not go beyond the end of the command buffer. In particular, the GetFlashTable function is called directly on the Command Buffer before the DataSize is check, leading to possible circumstances where the data immediately following the command buffer could be destroyed before returning a buffer size error.	5.5	More Details
CVE-2023-26400	Adobe Dimension version 3.4.8 (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 file.	5.5	More Details
CVE-2023-30608	sqlparse is a non-validating SQL parser module for Python. In affected versions the SQL parser contains a regular expression that is vulnerable to ReDoS (Regular Expression Denial of Service). This issue was introduced by commit `e75e358`. The vulnerability may lead to Denial of Service (DoS). This issues has been fixed in sqlparse 0.4.4 by commit `c457abd5f`. Users are advised to upgrade. There are no known workarounds for this issue.	5.5	More Details
CVE-2023-26404	Adobe Dimension version 3.4.8 (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 file.	5.5	More Details
CVE-2023-29573	Bento4 v1.6.0-639 was discovered to contain an out-of-memory bug in the mp4info component.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21929	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 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 as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	5.5	More Details
CVE-2022-46886	There exists an open redirect within the response list update functionality of ServiceNow. This allows attackers to redirect users to arbitrary domains when clicking on a URL within a service-now domain.	5.5	More Details
CVE-2023-28091	HPE OneView virtual appliance "Migrate server hardware" option may expose sensitive information in an HPE OneView support dump	5.5	More Details
CVE-2023-28085	An HPE OneView Global Dashboard (OVGD) appliance dump may expose OVGD user account credentials	5.5	More Details
CVE-2023-27610	Auth. (admin+) SQL Injection (SQLi) vulnerability in TransbankDevelopers Transbank Webpay REST plugin <= 1.6.6 versions.	5.5	More Details
CVE-2023-29569	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via ffi_cb_impl_wpwwwww at src/mjs_ffi.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2023-1548	A CWE-269: Improper Privilege Management vulnerability exists that could cause a local user to perform a denial of service through the console server service that is part of EcoStruxure Control Expert. Affected Products: EcoStruxure Control Expert (V15.1 and above)	5.5	More Details
CVE-2023-21926	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Health Sciences InForm executes to compromise Oracle Health Sciences InForm. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Health Sciences InForm accessible data. CVSS 3.1 Base Score 5.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N).	5.5	More Details
CVE-2022-48468	protobuf-c before 1.4.1 has an unsigned integer overflow in parse_required_member.	5.5	More Details
CVE-2023-26264	All versions of Talend Data Catalog before 8.0-20220907 are potentially vulnerable to XML External Entity (XXE) attacks in the license parsing code.	5.5	More Details
CVE-2023-26263	All versions of Talend Data Catalog before 8.0-20230110 are potentially vulnerable to XML External Entity (XXE) attacks in the /MIMBWebServices/license endpoint of the remote harvesting server.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25954	KYOCERA Mobile Print' v3.2.0.230119 and earlier, 'UTAX/TA MobilePrint' v3.2.0.230119 and earlier, and 'Olivetti Mobile Print' v3.2.0.230119 and earlier are vulnerable to improper intent handling. When a malicious app is installed on the victim user's Android device, the app may send an intent and direct the affected app to download malicious files or apps to the device without notification.	5.5	More Details
CVE-2023-26403	Adobe Substance 3D Stager version 2.0.1 (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 file.	5.5	More Details
CVE-2023-26387	Adobe Substance 3D Stager version 2.0.1 (and earlier) is affected by an Access of Uninitialized Pointer 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-2023-26386	Adobe Substance 3D Stager version 2.0.1 (and earlier) is affected by an Access of Uninitialized Pointer 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-2023-26385	Adobe Substance 3D Stager version 2.0.1 (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 file.	5.5	More Details
CVE-2023-1906	A heap-based buffer overflow issue was discovered in ImageMagick's ImportMultiSpectralQuantum() function in MagickCore/quantum-import.c. An attacker could pass specially crafted file to convert, triggering an out-of-bounds read error, allowing an application to crash, resulting in a denial of service.	5.5	More Details
CVE-2023-26397	Adobe Acrobat Reader versions 23.001.20093 (and earlier) and 20.005.30441 (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-2023-22307	Sensitive data exposure in Webconf in Tribe29 Checkmk Appliance before 1.6.4 allows local attacker to retrieve passwords via reading log files.	5.5	More Details
CVE-2023-30538	Discourse is an open source platform for community discussion. Due to the improper sanitization of SVG files, an attacker can execute arbitrary JavaScript on the users' browsers by uploading a crafted SVG file. This issue is patched in the latest stable and tests-passed versions of Discourse. Users are advised to upgrade. For users unable to upgrade there are two possible workarounds: enable CDN handing of uploads (and ensure the CDN sanitizes SVG files) or disable SVG file uploads by ensuring that the `authorized extensions` site setting does not include `svg` (or reset that setting to the default, by default Discourse doesn't enable SVG uploads by users).	5.4	More Details
CVE-2023-21921	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences InForm. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Health Sciences InForm accessible data as well as unauthorized read access to a subset of Oracle Health Sciences InForm 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 Number	Description	Base Score	Reference
CVE-2023-21973	Vulnerability in the Oracle iProcurement product of Oracle E-Business Suite (component: E-Content Manager Catalog). 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 iProcurement. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iProcurement, 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 iProcurement accessible data as well as unauthorized read access to a subset of Oracle iProcurement 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-2023-21936	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime SEC). Supported versions that are affected are Prior to 9.2.7.3. Easily exploitable vulnerability allows low privileged 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 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-2023-21992	Vulnerability in the PeopleSoft Enterprise HCM Human Resources product of Oracle PeopleSoft (component: Administer Workforce). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Human Resources. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HCM Human Resources accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HCM Human Resources 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-2022-45839	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in WHA WHA Puzzle plugin <= 1.0.9 versions.	5.4	More Details
CVE-2023-29774	Dreamer CMS 3.0.1 is vulnerable to stored Cross Site Scripting (XSS).	5.4	More Details
CVE-2023-2104	Improper Access Control in GitHub repository alextselegidis/easyappointments prior to 1.5.0.	5.4	More Details
CVE-2022-45358	Auth. (subscriber+) Reflected Cross-Site Scripting (XSS) vulnerability in Silkalns Activello theme <= 1.4.4 versions.	5.4	More Details
CVE-2022-47053	An arbitrary file upload vulnerability in the Digital Assets Manager module of DNN Corp DotNetNuke v7.0.0 to v9.10.2 allows attackers to execute arbitrary code via a crafted SVG file.	5.4	More Details
CVE-2018-17454	An issue was discovered in GitLab Community and Enterprise Edition before 11.1.7, 11.2.x before 11.2.4, and 11.3.x before 11.3.1. There is stored XSS on the issue details screen.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29506	XWiki Commons are technical libraries common to several other top level XWiki projects. It was possible to inject some code using the URL of authenticated endpoints. This problem has been patched on XWiki 13.10.11, 14.4.7 and 14.10.	5.4	More Details
CVE-2022-45849	Auth. (subscriber+) Reflected Cross-Site Scripting (XSS) vulnerability in Silkalns Activello theme <= 1.4.4 versions.	5.4	More Details
CVE-2023-27775	A stored HTML injection vulnerability in LiveAction LiveSP v21.1.2 allows attackers to execute arbitrary code via a crafted payload.	5.4	More Details
CVE-2022-44726	The TouchDown Timesheet tracking component 4.1.4 for Jira allows XSS in the calendar view.	5.4	More Details
CVE-2023-0367	The Pricing Tables For WPBakery Page Builder (formerly Visual Composer) WordPress plugin before 3.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2023-2103	Cross-site Scripting (XSS) - Stored in GitHub repository alextselegidis/easyappointments prior to 1.5.0.	5.4	More Details
CVE-2023-0374	The W4 Post List WordPress plugin before 2.4.6 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2023-0764	The Gallery by BestWebSoft WordPress plugin before 4.7.0 does not perform proper sanitization of gallery information, leading to a Stored Cross-Site Scription vulnerability. The attacker must have at least the privileges of the Author role.	5.4	More Details
CVE-2023-30520	Jenkins Quay.io trigger Plugin 0.1 and earlier does not limit URL schemes for repository homepage URLs submitted via Quay.io trigger webhooks, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to submit crafted Quay.io trigger webhook payloads.	5.4	More Details
CVE-2023-1325	The Easy Forms for Mailchimp WordPress plugin before 6.8.7 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2018-17537	An issue was discovered in GitLab Community and Enterprise Edition before 11.1.7, 11.2.x before 11.2.4, and 11.3.x before 11.3.1. blog-viewer has stored XSS during repository browsing, if package.json exists. .	5.4	More Details
CVE-2022-48178	X2CRM Open Source Sales CRM 6.6 and 6.9 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Create Action function, aka an index.php/actions/update URI.	5.4	More Details
CVE-2018-17536	An issue was discovered in GitLab Community and Enterprise Edition before 11.1.7, 11.2.x before 11.2.4, and 11.3.x before 11.3.1. There is stored XSS on the merge request page via project import.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48177	X2CRM Open Source Sales CRM 6.6 and 6.9 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the adin/importModels Import Records Model field (model parameter). This vulnerability allows attackers to create malicious JavaScript that will be executed by the victim user's browser.	5.4	More Details
CVE-2023-2021	Cross-site Scripting (XSS) - Stored in GitHub repository nilsteampassnet/teampass prior to 3.0.3.	5.4	More Details
CVE-2023-27890	The Export User plugin through 2.0 for MyBB allows XSS during the process of an admin generating DSGVO data for a user, via the Custom User Title, Location, or Bio field. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	5.4	More Details
CVE-2023-29847	AeroCMS v0.0.1 was discovered to contain multiple stored cross-site scripting (XSS) vulnerabilities via the comment_author and comment_content parameters at /post.php. These vulnerabilities allow attackers to execute arbitrary web scripts or HTML via a crafted payload.	5.4	More Details
CVE-2023-26559	A directory traversal vulnerability in Oxygen XML Web Author before 25.0.0.3 build 2023021715 and Oxygen Content Fusion before 5.0.3 build 2023022015 allows an attacker to read files from a WEB-INF directory via a crafted HTTP request. (XML Web Author 24.1.0.3 build 2023021714 and 23.1.1.4 build 2023021715 are also fixed versions.)	5.3	More Details
CVE-2018-17453	An issue was discovered in GitLab Community and Enterprise Edition before 11.1.7, 11.2.x before 11.2.4, and 11.3.x before 11.3.1. Attackers may have been able to obtain sensitive access-token data from Sentry logs via the GRPC::Unknown exception.	5.3	More Details
CVE-2023-21903	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: OBVAM Internal Tfr Domain). Supported versions that are affected are 14.5, 14.6 and 14.7. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Virtual Account Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Virtual Account Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Virtual Account Management. CVSS 3.1 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:L).	5.3	More Details
CVE-2023-21904	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: OBVAM Trn Journal Domain). Supported versions that are affected are 14.5, 14.6 and 14.7. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Virtual Account Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Virtual Account Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Virtual Account Management. CVSS 3.1 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:L).	5.3	More Details
CVE-2023-30517	Jenkins NeuVector Vulnerability Scanner Plugin 1.22 and earlier unconditionally disables SSL/TLS certificate and hostname validation when connecting to a configured NeuVector Vulnerability Scanner server.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29132	Irssi 1.3.x and 1.4.x before 1.4.4 has a use-after-free because of use of a stale special collector reference. This occurs when printing of a non-formatted line is concurrent with printing of a formatted line.	5.3	More Details
CVE-2023-21971	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.0.32 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Connectors. 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 MySQL Connectors as well as unauthorized update, insert or delete access to some of MySQL Connectors accessible data and unauthorized read access to a subset of MySQL Connectors accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:H).	5.3	More Details
CVE-2023-24511	On affected platforms running Arista EOS with SNMP configured, a specially crafted packet can cause a memory leak in the snmpd process. This may result in the snmpd processing being terminated (causing SNMP requests to time out until snmpd is automatically restarted) and potential memory resource exhaustion for other processes on the switch. The vulnerability does not have any confidentiality or integrity impacts to the system.	5.3	More Details
CVE-2023-26048	Jetty is a java based web server and servlet engine. In affected versions servlets with multipart support (e.g. annotated with `@MultipartConfig`) that call `HttpServletRequest.getParameter()` or `HttpServletRequest.getParts()` may cause `OutOfMemoryError` when the client sends a multipart request with a part that has a name but no filename and very large content. This happens even with the default settings of `fileSizeThreshold=0` which should stream the whole part content to disk. An attacker client may send a large multipart request and cause the server to throw `OutOfMemoryError`. However, the server may be able to recover after the `OutOfMemoryError` and continue its service -- although it may take some time. This issue has been patched in versions 9.4.51, 10.0.14, and 11.0.14. Users are advised to upgrade. Users unable to upgrade may set the multipart parameter `maxRequestSize` which must be set to a non-negative value, so the whole multipart content is limited (although still read into memory).	5.3	More Details
CVE-2023-30521	A missing permission check in Jenkins Assembla merge request builder Plugin 1.1.13 and earlier allows unauthenticated attackers to trigger builds of jobs corresponding to the attacker-specified repository.	5.3	More Details
CVE-2023-21944	Vulnerability in Oracle Essbase (component: Security and Provisioning). The supported version that is affected is 21.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Essbase. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Essbase accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N).	5.3	More Details
CVE-2023-21916	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Web Server). Supported versions that are affected are 8.58, 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 read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2023-30519	A missing permission check in Jenkins Quay.io trigger Plugin 0.1 and earlier allows unauthenticated attackers to trigger builds of jobs corresponding to the attacker-specified repository.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21943	Vulnerability in Oracle Essbase (component: Security and Provisioning). The supported version that is affected is 21.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Essbase. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Essbase accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N).	5.3	More Details
CVE-2023-21942	Vulnerability in Oracle Essbase (component: Security and Provisioning). The supported version that is affected is 21.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Essbase. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Essbase accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N).	5.3	More Details
CVE-2023-21939	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).	5.3	More Details
CVE-2023-30541	OpenZeppelin Contracts is a library for secure smart contract development. A function in the implementation contract may be inaccessible if its selector clashes with one of the proxy's own selectors. Specifically, if the clashing function has a different signature with incompatible ABI encoding, the proxy could revert while attempting to decode the arguments from calldata. The probability of an accidental clash is negligible, but one could be caused deliberately and could cause a reduction in availability. The issue has been fixed in version 4.8.3. As a workaround if a function appears to be inaccessible for this reason, it may be possible to craft the calldata such that ABI decoding does not fail at the proxy and the function is properly proxied through.	5.3	More Details
CVE-2023-27571	An issue was discovered in DG3450 Cable Gateway AR01.02.056.18_041520_711.NCS.10. The troubleshooting_logs_download.php log file download functionality does not check the session cookie. Thus, an attacker can download all log files.	5.3	More Details
CVE-2023-21925	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Health Sciences InForm. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Health Sciences InForm. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	5.3	More Details
CVE-2022-48437	An issue was discovered in x509/x509_verify.c in LibreSSL before 3.6.1, and in OpenBSD before 7.2 errata 001. x509_verify_ctx_add_chain does not store errors that occur during leaf certificate verification, and therefore an incorrect error is returned. This behavior occurs when there is an installed verification callback that instructs the verifier to continue upon detecting an invalid certificate.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29197	guzzlehttp/psr7 is a PSR-7 HTTP message library implementation in PHP. Affected versions are subject to improper header parsing. An attacker could sneak in a newline (\n) into both the header names and values. While the specification states that \r\n\r\n is used to terminate the header list, many servers in the wild will also accept \n\n. This is a follow-up to CVE-2022-24775 where the fix was incomplete. The issue has been patched in versions 1.9.1 and 2.4.5. There are no known workarounds for this vulnerability. Users are advised to upgrade.	5.3	More Details
CVE-2023-28963	An Improper Authentication vulnerability in cert-mgmt.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to read arbitrary files from temporary folders on the device. This issue affects Juniper Networks Junos OS: 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-S11; 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-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2.	5.3	More Details
CVE-2023-2152	A vulnerability has been found in SourceCodester Student Study Center Desk Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file index.php. The manipulation of the argument page leads to file inclusion. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-226273 was assigned to this vulnerability.	5.3	More Details
CVE-2023-28984	A Use After Free vulnerability in the Layer 2 Address Learning Manager (l2alm) of Juniper Networks Junos OS on QFX Series allows an adjacent attacker to cause the Packet Forwarding Engine to crash and restart, leading to a Denial of Service (DoS). The PFE may crash when a lot of MAC learning and aging happens, but due to a Race Condition (Concurrent Execution using Shared Resource with Improper Synchronization) that is outside the attackers direct control. This issue affects: Juniper Networks Junos OS versions prior to 19.4R3-S10 on QFX Series; 20.2 versions prior to 20.2R3-S7 on QFX Series; 20.3 versions prior to 20.3R3-S6 on QFX Series; 20.4 versions prior to 20.4R3-S5 on QFX Series; 21.1 versions prior to 21.1R3-S4 on QFX Series; 21.2 versions prior to 21.2R3-S3 on QFX Series; 21.3 versions prior to 21.3R3-S3 on QFX Series; 21.4 versions prior to 21.4R3 on QFX Series; 22.1 versions prior to 22.1R3 on QFX Series; 22.2 versions prior to 22.2R2 on QFX Series.	5.3	More Details
CVE-2023-28968	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX 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-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later 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-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2;	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28978	An Insecure Default Initialization of Resource vulnerability in Juniper Networks Junos OS Evolved allows an unauthenticated, network based attacker to read certain confidential information. In the default configuration it is possible to read confidential information about locally configured (administrative) users of the affected system. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S7-EVO on pending commit???; 21.1-EVO versions prior to 21.1R3-S4-EVO on awaiting build; 21.4-EVO versions prior to 21.4R3-S1-EVO; 22.2-EVO versions prior to 22.2R3-EVO; 21.2-EVO versions prior to 21.2R3-S5-EVO on pending commit???; 21.3-EVO version 21.3R1-EVO and later versions; 22.1-EVO version 22.1R1-EVO and later versions; 22.2-EVO versions prior to 22.2R2-S1-EVO.	5.3	More Details
CVE-2022-30076	ENTAB ERP 1.0 allows attackers to discover users' full names via a brute force attack with a series of student usernames such as s10000 through s20000. There is no rate limiting.	5.3	More Details
CVE-2023-28962	An Improper Authentication vulnerability in upload-file.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to upload arbitrary files to temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S11; 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-S6; 21.1 version 21.1R1 and later versions; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2.	5.3	More Details
CVE-2023-30543	@web3-react is a framework for building Ethereum Apps . In affected versions the `chainId` may be outdated if the user changes chains as part of the connection flow. This means that the value of `chainId` returned by `useWeb3React()` may be incorrect. In an application, this means that any data derived from `chainId` could be incorrect. For example, if a swapping application derives a wrapped token contract address from the `chainId` *and* a user has changed chains as part of their connection flow the application could cause the user to send funds to the incorrect address when wrapping. This issue has been addressed in PR #749 and is available in updated npm artifacts. There are no known workarounds for this issue. Users are advised to upgrade.	5.2	More Details
CVE-2023-29529	matrix-js-sdk is the Matrix Client-Server SDK for JavaScript and TypeScript. An attacker present in a room where an MSC3401 group call is taking place can eavesdrop on the video and audio of participants using matrix-js-sdk, without their knowledge. To affected matrix-js-sdk users, the attacker will not appear to be participating in the call. This attack is possible because matrix-js-sdk's group call implementation accepts incoming direct calls from other users, even if they have not yet declared intent to participate in the group call, as a means of resolving a race condition in call setup. Affected versions do not restrict access to the user's outbound media in this case. Legacy 1:1 calls are unaffected. This is fixed in matrix-js-sdk 24.1.0. As a workaround, users may hold group calls in private rooms where only the exact users who are expected to participate in the call are present.	5.0	More Details
CVE-2023-21933	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 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-2023-22949	An issue was discovered in TigerGraph Enterprise Free Edition 3.x. There is logging of user credentials. All authenticated GSQL access requests are logged by TigerGraph in multiple places. Each request includes both the username and password of the user in an easily decodable base64 form. That could allow a TigerGraph administrator to effectively harvest usernames/passwords.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21935	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 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-2023-21919	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 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-2023-25504	A malicious actor who has been authenticated and granted specific permissions in Apache Superset may use the import dataset feature in order to conduct Server-Side Request Forgery attacks and query internal resources on behalf of the server where Superset is deployed. This vulnerability exists in Apache Superset versions up to and including 2.0.1.	4.9	More Details
CVE-2023-21972	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 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-2023-21945	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 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-2023-21976	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 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-2023-21920	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 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-2023-1427	- The Photo Gallery by 10Web WordPress plugin before 1.8.15 did not ensure that uploaded files are kept inside its uploads folder, allowing high privilege users to put images anywhere in the filesystem via a path traversal vector.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21966	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: JSON). Supported versions that are affected are 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-2023-21917	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 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-2023-21953	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 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-2023-21982	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 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-2023-21981	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Elastic Search). Supported versions that are affected are 8.58, 8.59 and 8.60. Easily exploitable vulnerability allows high privileged 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 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	4.9	More Details
CVE-2023-22948	An issue was discovered in TigerGraph Enterprise Free Edition 3.x. There is unsecured read access to an SSH private key. Any code that runs as the tigergraph user is able to read the SSH private key. With this, an attacker is granted password-less SSH access to all machines in the TigerGraph cluster.	4.9	More Details
CVE-2023-23591	The Logback component in Terminalfour before 8.3.14.1 allows OS administrators to obtain sensitive information from application server logs when debug logging is enabled. The fixed versions are 8.2.18.7, 8.2.18.2.2, 8.3.11.1, and 8.3.14.1.	4.9	More Details
CVE-2023-21955	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 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 Number	Description	Base Score	Reference
CVE-2023-21911	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 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-2023-21977	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 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-2023-21913	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 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-2023-21962	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 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-2023-2102	Cross-site Scripting (XSS) - Stored in GitHub repository alextselegidis/easyappointments prior to 1.5.0.	4.8	More Details
CVE-2022-44735	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Gus Sevilla WP Clictracker plugin <= 1.0.5 versions.	4.8	More Details
CVE-2023-2014	Cross-site Scripting (XSS) - Generic in GitHub repository microweber/microweber prior to 1.3.3.	4.8	More Details
CVE-2022-44734	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in BestWebSoft Car Rental by BestWebSoft plugin <= 1.1.2 versions.	4.8	More Details
CVE-2022-43480	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Magneticlab Sàrl Homepage Pop-up plugin <= 1.2.5 versions.	4.8	More Details
CVE-2022-44632	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Denis Buka Content Repeater – Custom Posts Simplified plugin <= 1.1.13 versions.	4.8	More Details
CVE-2022-44625	Auth. (admin+) Stored Cross-Site Scripting') vulnerability in Zephilou Cyklodev WP Notify plugin <= 1.2.1 versions.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1990	A use-after-free flaw was found in ndlc_remove in drivers/nfc/st-nci/ndlc.c in the Linux Kernel. This flaw could allow an attacker to crash the system due to a race problem.	4.7	More Details
CVE-2023-28979	An Improper Check for Unusual or Exceptional Conditions vulnerability in the kernel of Juniper Networks Junos OS allows an adjacent unauthenticated attacker to bypass an integrity check. In a 6PE scenario and if an additional integrity check is configured, it will fail to drop specific malformed IPv6 packets, and then these packets will be forwarded to other connected networks. This issue affects Juniper Networks Junos OS: All versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R3-S1; 21.4 versions prior to 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R2; 22.2 versions prior to 22.2R2.	4.7	More Details
CVE-2023-2150	A vulnerability, which was classified as critical, has been found in SourceCodester Task Reminder System 1.0. This issue affects some unknown processing of the file Master.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-226271.	4.7	More Details
CVE-2023-2154	A vulnerability was found in SourceCodester Task Reminder System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/?page=reminders/view_reminder. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-226275.	4.7	More Details
CVE-2023-29204	XWiki Commons are technical libraries common to several other top level XWiki projects. It is possible to bypass the existing security measures put in place to avoid open redirect by using a redirect such as `//mydomain.com` (i.e. omitting the `http:`). It was also possible to bypass it when using URL such as `http:/mydomain.com`. The problem has been patched on XWiki 13.10.10, 14.4.4 and 14.8RC1.	4.7	More Details
CVE-2023-21998	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, 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 VM VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data. Note: This vulnerability applies to Windows VMs only. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N).	4.6	More Details
CVE-2023-28975	An Unexpected Status Code or Return Value vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated attacker with physical access to the device to cause a Denial of Service (DoS). When certain USB devices are connected to a USB port of the routing-engine (RE), the kernel will crash leading to a reboot of the device. The device will continue to crash as long as the USB device is connected. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S10; 20.2 versions prior to 20.2R3-S7; 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-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2, 22.2R3; 22.3 versions prior to 22.3R1-S1, 22.3R2; 22.4 versions prior to 22.4R2.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22000	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, 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 VM VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N).	4.6	More Details
CVE-2023-21915	Vulnerability in the Oracle Banking Payments product of Oracle Financial Services Applications (component: Book/Internal Transfer). Supported versions that are affected are 14.5, 14.6 and 14.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. 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 Banking Payments accessible data as well as unauthorized read access to a subset of Oracle Banking Payments accessible data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N).	4.6	More Details
CVE-2023-22001	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, 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 VM VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N).	4.6	More Details
CVE-2023-21940	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.32 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-2023-21947	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.32 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-2023-21997	Vulnerability in the Oracle User Management product of Oracle E-Business Suite (component: Proxy User Delegation). 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 User Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle User Management 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-2021-41613	An issue was discovered in the controller unit of the OpenRISC mor1kx processor. The write logic of Exception Effective Address Register (EEAR) is not implemented correctly. User programs from authorized privilege levels will be unable to write to EEAR.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21959	Vulnerability in the Oracle iReceivables product of Oracle E-Business Suite (component: Attachments). 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 iReceivables. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle iReceivables 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-2023-30529	Jenkins Lucene-Search Plugin 387.v938a_ecb_f7fe9 and earlier does not require POST requests for an HTTP endpoint, allowing attackers to reindex the database.	4.3	More Details
CVE-2023-30518	A missing permission check in Jenkins Thycotic Secret Server Plugin 1.0.2 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details
CVE-2023-30530	Jenkins Consul KV Builder Plugin 2.0.13 and earlier stores the HashiCorp Consul ACL Token unencrypted in its global configuration file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.	4.3	More Details
CVE-2023-2059	A vulnerability was found in DedeCMS 5.7.87. It has been rated as problematic. Affected by this issue is some unknown functionality of the file uploads/include/dialog/select_templets.php. The manipulation leads to path traversal: '..\filedir'. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-225944.	4.3	More Details
CVE-2023-30474	Cross-Site Request Forgery (CSRF) vulnerability in Kilian Evang Ultimate Noindex Nofollow Tool II plugin <= 1.3 versions.	4.3	More Details
CVE-2018-17450	An issue was discovered in GitLab Community and Enterprise Edition before 11.1.7, 11.2.x before 11.2.4, and 11.3.x before 11.3.1. There is Server-Side Request Forgery (SSRF) via the Kubernetes integration, leading (for example) to disclosure of a GCP service token.	4.3	More Details
CVE-2023-21902	Vulnerability in the Oracle Financial Services Behavior Detection Platform product of Oracle Financial Services Applications (component: Application). The supported version that is affected is 8.0.8.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Behavior Detection Platform. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Financial Services Behavior Detection Platform 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-2021-30153	An issue was discovered in the VisualEditor extension in MediaWiki before 1.31.13, and 1.32.x through 1.35.x before 1.35.2. . When using VisualEditor to edit a MediaWiki user page belonging to an existing, but hidden, user, VisualEditor will disclose that the user exists. (It shouldn't because they are hidden.) This is related to ApiVisualEditor.	4.3	More Details
CVE-2023-2101	A vulnerability, which was classified as problematic, has been found in moxi624 Mogu Blog v2 up to 5.2. This issue affects the function uploadPictureByUrl of the file /mogu-picture/file/uploadPicsByUrl. The manipulation of the argument urlList leads to absolute path traversal. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-226109 was assigned to this vulnerability.	4.3	More Details
CVE-2022-43699	OX App Suite before 7.10.6-rev30 allows SSRF because e-mail account discovery disregards the deny-list and thus can be attacked by an adversary who controls the DNS records of an external domain (found in the host part of an e-mail address).	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43698	OX App Suite before 7.10.6-rev30 allows SSRF because changing a POP3 account disregards the deny-list.	4.3	More Details
CVE-2023-21927	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Interoperability SEC). Supported versions that are affected are Prior to 9.2.7.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of JD Edwards EnterpriseOne Tools 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-2023-30522	A missing permission check in Jenkins Fogbugz Plugin 2.2.17 and earlier allows attackers with Item/Read permission to trigger builds of jobs specified in a 'jobname' request parameter.	4.3	More Details
CVE-2023-30523	Jenkins Report Portal Plugin 0.5 and earlier stores ReportPortal access tokens unencrypted in job config.xml files on the Jenkins controller as part of its configuration where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	4.3	More Details
CVE-2023-30524	Jenkins Report Portal Plugin 0.5 and earlier does not mask ReportPortal access tokens displayed on the configuration form, increasing the potential for attackers to observe and capture them.	4.3	More Details
CVE-2023-30527	Jenkins WSO2 Oauth Plugin 1.0 and earlier stores the WSO2 Oauth client secret unencrypted in the global config.xml file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.	4.3	More Details
CVE-2023-30548	gatsby-plugin-sharp is a plugin for the gatsby framework which exposes functions built on the Sharp image processing library. The gatsby-plugin-sharp plugin prior to versions 5.8.1 and 4.25.1 contains a path traversal vulnerability exposed when running the Gatsby develop server (`gatsby develop`). It should be noted that by default gatsby develop is only accessible via the localhost 127.0.0.1, and one would need to intentionally expose the server to other interfaces to exploit this vulnerability by using server options such as --host 0.0.0.0, -H 0.0.0.0, or the GATSBY_HOST=0.0.0.0 environment variable. Attackers exploiting this vulnerability will have read access to all files within the scope of the server process. A patch has been introduced in gatsby-plugin-sharp@5.8.1 and gatsby-plugin-sharp@4.25.1 which mitigates the issue by ensuring that included paths remain within the project directory. As stated above, by default gatsby develop is only exposed to the localhost 127.0.0.1. For those using the develop server in the default configuration no risk is posed. If other ranges are required, preventing the develop server from being exposed to untrusted interfaces or IP address ranges would mitigate the risk from this vulnerability. Users are non the less encouraged to upgrade to a safe version.	4.3	More Details
CVE-2023-21941	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Web Server). Supported versions that are affected are 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle BI Publisher 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-2023-2020	Insufficient permission checks in the REST API in Tribe29 Checkmk <= 2.1.0p27 and <= 2.2.0b4 (beta) allow unauthorized users to schedule downtimes for any host.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30606	Discourse is an open source platform for community discussion. In affected versions a user logged as an administrator can call arbitrary methods on the `SiteSetting` class, notably `#clear_cache!` and `#notify_changed!`, which when done on a multisite instance, can affect the entire cluster resulting in a denial of service. Users not running in multisite environments are not affected. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.2	More Details
CVE-2023-29196	Discourse is an open source platform for community discussion. This vulnerability is not exploitable on the default install of Discourse. A custom feature must be enabled for it to work at all, and the attacker's payload must pass the CSP to be executed. However, if an attacker succeeds in embedding Javascript that does pass the CSP, it could result in session hijacking for any users that view the attacker's post. The vulnerability is patched in the latest tests-passed, beta and stable branches. Users are advised to upgrade. Users unable to upgrade should enable and/or restore your site's CSP to the default one provided with Discourse. Remove any embeddable hosts configured.	4.2	More Details
CVE-2022-43458	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in Code Tides Advanced Floating Content plugin <= 1.2.1 versions.	4.1	More Details
CVE-2023-29194	Vitess is a database clustering system for horizontal scaling of MySQL. Users can either intentionally or inadvertently create a keyspace containing `/` characters such that from that point on, anyone who tries to view keyspaces from VTAdmin will receive an error. Trying to list all the keyspaces using `vtctldclient GetKeyspaces` will also return an error. Note that all other keyspaces can still be administered using the CLI (vtctldclient). This issue is fixed in version 16.0.1. As a workaround, delete the offending keyspace using a CLI client (vtctldclient).	4.1	More Details
CVE-2023-0005	A vulnerability in Palo Alto Networks PAN-OS software enables an authenticated administrator to expose the plaintext values of secrets stored in the device configuration and encrypted API keys.	4.1	More Details
CVE-2023-21988	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	3.8	More Details
CVE-2023-21937	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. 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-2023-21938	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition 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 3.7 (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-2023-22687	Insecure Storage of Sensitive Information vulnerability in Jose Mortellaro Freesoul Deactivate Plugins – Plugin manager and cleanup plugin <= 1.9.4.0 versions.	3.7	More Details
CVE-2023-29203	XWiki Commons are technical libraries common to several other top level XWiki projects. It's possible to list some users who are normally not viewable from subwiki by requesting users on a subwiki which allows only global users with `uorgsuggest.vm`. This issue only concerns hidden users from main wiki. Note that the disclosed information are the username and the first and last name of users, no other information is leaked. The problem has been patched on XWiki 13.10.8, 14.4.3 and 14.7RC1.	3.7	More Details
CVE-2023-21968	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. 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-2023-21999	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Difficult to exploit 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 update, insert or delete access to some of Oracle VM VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N).	3.6	More Details
CVE-2023-2077	A vulnerability, which was classified as problematic, has been found in Campcodes Online Traffic Offense Management System 1.0. This issue affects some unknown processing of the file /admin/offenses/view_details.php. The manipulation of the argument id leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-226055.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2153	A vulnerability was found in SourceCodester Complaint Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file admin/assets/plugins/DataTables/examples/examples_support/editable_ajax.php of the component POST Parameter Handler. The manipulation of the argument value with the input 1> <script>alert(666)</script> leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-226274 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2015-10101	A vulnerability classified as problematic was found in Google Analytics Top Content Widget Plugin up to 1.5.6 on WordPress. Affected by this vulnerability is an unknown functionality of the file class-tgm-plugin-activation.php. The manipulation leads to cross site scripting. The attack can be launched remotely. Upgrading to version 1.5.7 is able to address this issue. The identifier of the patch is 25bb1dea113716200a6f0f3135801d84a7a65540. It is recommended to upgrade the affected component. The identifier VDB-226117 was assigned to this vulnerability.	3.5	More Details
CVE-2023-2100	A vulnerability classified as problematic was found in SourceCodester Vehicle Service Management System 1.0. This vulnerability affects unknown code of the file /admin/report/index.php. The manipulation of the argument date_end leads to cross site scripting. 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-226108.	3.5	More Details
CVE-2023-2099	A vulnerability classified as problematic has been found in SourceCodester Vehicle Service Management System 1.0. This affects an unknown part of the file /classes/Users.php. The manipulation of the argument id leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-226107.	3.5	More Details
CVE-2023-2098	A vulnerability was found in SourceCodester Vehicle Service Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /inc/topBarNav.php. The manipulation of the argument search leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-226106 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-2076	A vulnerability classified as problematic was found in Campcodes Online Traffic Offense Management System 1.0. This vulnerability affects unknown code of the file /classes/Users.phpp. The manipulation of the argument id leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-226054 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-30540	Nextcloud Talk is a chat, video & audio call extension for Nextcloud. In affected versions a user that was added later to a conversation can use this information to get access to data that was deleted before they were added to the conversation. This issue has been patched in version 15.0.5 and it is recommended that users upgrad to 15.0.5. There are no known workarounds for this issue.	3.5	More Details
CVE-2023-2055	A vulnerability has been found in Campcodes Advanced Online Voting System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/config_save.php. The manipulation of the argument title leads to cross site scripting. 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-225940.	3.5	More Details
CVE-2023-2044	A vulnerability has been found in Control iD iDSecure 4.7.29.1 and classified as problematic. This vulnerability affects unknown code of the component Dispositivos Page. The manipulation of the argument IP-DNS leads to cross site scripting. The attack can be initiated remotely. VDB-225922 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 Number	Description	Base Score	Reference
CVE-2023-22003	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Utility). Supported versions that are affected are 10 and 11. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. 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 Solaris accessible data. CVSS 3.1 Base Score 3.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).	3.3	More Details
CVE-2023-27703	The Android version of pikpak v1.29.2 was discovered to contain an information leak via the debug interface.	3.3	More Details
CVE-2023-29383	In Shadow 4.13, it is possible to inject control characters into fields provided to the SUID program chfn (change finger). Although it is not possible to exploit this directly (e.g., adding a new user fails because \n is in the block list), it is possible to misrepresent the /etc/passwd file when viewed. Use of \r manipulations and Unicode characters to work around blocking of the : character make it possible to give the impression that a new user has been added. In other words, an adversary may be able to convince a system administrator to take the system offline (an indirect, social-engineered denial of service) by demonstrating that "cat /etc/passwd" shows a rogue user account.	3.3	More Details
CVE-2023-21991	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N).	3.2	More Details
CVE-2023-27525	An authenticated user with Gamma role authorization could have access to metadata information using non trivial methods in Apache Superset up to and including 2.0.1	3.1	More Details
CVE-2015-10103	A vulnerability, which was classified as problematic, was found in InternalError503 Forget It up to 1.3. This affects an unknown part of the file js/settings.js. The manipulation of the argument setForgetTime with the input 0 leads to infinite loop. It is possible to launch the attack on the local host. Upgrading to version 1.4 is able to address this issue. The patch is named adf0c7fd59b9c935b4fd675c556265620124999c. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-226119.	2.8	More Details
CVE-2023-21963	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Connection Handling). Supported versions that are affected are 5.7.40 and prior and 8.0.31 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 partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).	2.7	More Details
CVE-2023-28440	Discourse is an open source platform for community discussion. In affected versions a maliciously crafted request from a Discourse administrator can lead to a long-running request and eventual timeout. This has the greatest potential impact in shared hosting environments where admins are untrusted. This issue has been addressed in versions 3.0.3 and 3.1.0.beta4. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2057	A vulnerability was found in EyouCms 1.5.4. It has been classified as problematic. Affected is an unknown function of the file login.php?m=admin&c=Arctype&a=edit of the component New Picture Handler. The manipulation of the argument litpic_loca leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-225942 is the identifier assigned to this vulnerability.	2.4	More Details
CVE-2023-2155	A vulnerability was found in SourceCodester Air Cargo Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file classes/Master.php?f=save_cargo_type. The manipulation of the argument name leads to cross site scripting. 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-226276.	2.4	More Details
CVE-2023-2058	A vulnerability was found in EyouCms up to 1.6.2. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /yxcms/index.php?r=admin/extendfield/mesedit&tabid=12&id=4 of the component HTTP POST Request Handler. The manipulation of the argument web_ico leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-225943.	2.4	More Details
CVE-2023-26049	Jetty is a java based web server and servlet engine. Nonstandard cookie parsing in Jetty may allow an attacker to smuggle cookies within other cookies, or otherwise perform unintended behavior by tampering with the cookie parsing mechanism. If Jetty sees a cookie VALUE that starts with `"` (double quote), it will continue to read the cookie string until it sees a closing quote -- even if a semicolon is encountered. So, a cookie header such as: `DISPLAY_LANGUAGE="b; JSESSIONID=1337; c=d"` will be parsed as one cookie, with the name DISPLAY_LANGUAGE and a value of b; JSESSIONID=1337; c=d instead of 3 separate cookies. This has security implications because if, say, JSESSIONID is an HttpOnly cookie, and the DISPLAY_LANGUAGE cookie value is rendered on the page, an attacker can smuggle the JSESSIONID cookie into the DISPLAY_LANGUAGE cookie and thereby exfiltrate it. This is significant when an intermediary is enacting some policy based on cookies, so a smuggled cookie can bypass that policy yet still be seen by the Jetty server or its logging system. This issue has been addressed in versions 9.4.51, 10.0.14, 11.0.14, and 12.0.0.beta0 and users are advised to upgrade. There are no known workarounds for this issue.	2.4	More Details
CVE-2023-21928	Vulnerability in the Oracle Solaris product of Oracle Systems (component: IPS repository daemon). The supported version that is affected is 11. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. 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 Solaris accessible data. CVSS 3.1 Base Score 1.8 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:N).	1.8	More Details
CVE-2023-1271	Rejected reason: Duplicate. Please use CVE-2023-24421.	N/A	More Details
CVE-2023-1706	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2022-43128	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2022-42245. Reason: This record is a duplicate of CVE-2022-42245. Notes: All CVE users should reference CVE-2022-42245 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4463	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2023-2004	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-2023-1842	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-2022-3404	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2022-4893	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-2022-2445	Rejected reason: Incorrectly assigned CVE. Not a valid issue.	N/A	More Details