SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 08 March 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-2023-26477	XWiki Platform is a generic wiki platform. Starting in versions 6.3-rc-1 and 6.2.4, it's possible to inject arbitrary wiki syntax including Groovy, Python and Velocity script macros via the `newThemeName` request parameter (URL parameter), in combination with additional parameters. This has been patched in the supported versions 13.10.10, 14.9-rc-1, and 14.4.6. As a workaround, it is possible to edit `FlamingoThemesCode.WebHomeSheet` and manually perform the changes from the patch fixing the issue.	10.0	More Details
CVE-2023-27479	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions any user with view 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 UIX parameters. A proof of concept exploit is to log in, add an `XWiki.UIExtensionClass` xobject to the user profile page, with an Extension Parameters content containing `label={{/html}} {{async async="true" cached="false" context="doc.reference"}}{{groovy}}println("Hello " + "from groovy!"){{/groovy}} {{/async}}`. Then, navigating to `PanelsCode.ApplicationsPanelConfigurationSheet` (i.e., `<xwiki-host>/xwiki/bin/view/PanelsCode/ApplicationsPanelConfigurationSheet` where `<xwiki-host>` is the URL of your XWiki installation) should not execute the Groovy script. If it does, you will see `Hello from groovy!` displayed on the screen. This vulnerability has been patched in XWiki 13.10.11, 14.4.7 and 14.10-rc-1. Users are advised to upgrade. For users unable to upgrade the issue can be fixed by editing the `PanelsCode.ApplicationsPanelConfigurationSheet` wiki page and making the same modifications as shown in commit `6de5442f3c`.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26475	XWiki Platform is a generic wiki platform. Starting in version 2.3-milestone-1, the annotation displayer does not execute the content in a restricted context. This allows executing anything with the right of the author of any document by annotating the document. This has been patched in XWiki 13.10.11, 14.4.7 and 14.10. There is no easy workaround except to upgrade.	9.9	More Details
CVE-2023-26474	XWiki Platform is a generic wiki platform. Starting in version 13.10, it's possible to use the right of an existing document content author to execute a text area property. This has been patched in XWiki 14.10, 14.4.7, and 13.10.11. There are no known workarounds.	9.9	More Details
CVE-2023-26472	XWiki Platform is a generic wiki platform. Starting in version 6.2-milestone-1, one can execute any wiki content with the right of IconThemeSheet author by creating an icon theme with certain content. This can be done by creating a new page or even through the user profile for users not having edit right. The issue has been patched in XWiki 14.9, 14.4.6, and 13.10.10. An available workaround is to fix the bug in the page `IconThemesCode.IconThemeSheet` by applying a modification from commit 48caf7491595238af2b531026a614221d5d61f38.	9.9	More Details
CVE-2023-26471	XWiki Platform is a generic wiki platform. Starting in version 11.6-rc-1, comments are supposed to be executed with the right of superadmin but in restricted mode (anything dangerous is disabled), but the async macro does not take into account the restricted mode. This means that any user with comment right can use the async macro to make it execute any wiki content with the right of superadmin. This has been patched in XWiki 14.9, 14.4.6, and 13.10.10. The only known workaround consists of applying a patch and rebuilding and redeploying `org.xwiki.platform:xwiki-platform-rendering-async-macro`.	9.9	More Details
CVE-2023-26055	XWiki Commons are technical libraries common to several other top level XWiki projects. Starting in version 3.1-milestone-1, any user can edit their own profile and inject code, which is going to be executed with programming right. The same vulnerability can also be exploited in all other places where short text properties are displayed, e.g., in apps created using Apps Within Minutes that use a short text field. The problem has been patched on versions 13.10.9, 14.4.4, 14.7RC1.	9.9	More Details
CVE-2023-24643	Judging Management System v1.0 was discovered to contain a SQL injection vulnerability via the sid parameter at /php-jms/updateBlankTxtview.php.	9.8	More Details
CVE-2023-27574	ShadowsocksX-NG 1.10.0 signs with com.apple.security.get-task-allow entitlements because of CODE_SIGNING_INJECT_BASE_ENTITLEMENTS.	9.8	More Details
CVE-2023-26779	CleverStupidDog yf-exam v 1.8.0 is vulnerable to Deserialization which can lead to remote code execution (RCE).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22336	Path traversal vulnerability in SS1 Ver.13.0.0.40 and earlier and Rakuraku PC Cloud Agent Ver.2.1.8 and earlier allows a remote attacker to upload a specially crafted file to an arbitrary directory. As a result of exploiting this vulnerability with CVE-2023-22335 and CVE-2023-22344 vulnerabilities together, it may allow a remote attacker to execute an arbitrary code with SYSTEM privileges by sending a specially crafted script to the affected device.	9.8	More Details
CVE-2023-22344	Use of hard-coded credentials vulnerability in SS1 Ver.13.0.0.40 and earlier and Rakuraku PC Cloud Agent Ver.2.1.8 and earlier allows a remote attacker to obtain the password of the debug tool and execute it. As a result of exploiting this vulnerability with CVE-2023-22335 and CVE-2023-22336 vulnerabilities together, it may allow a remote attacker to execute an arbitrary code with SYSTEM privileges by sending a specially crafted script to the affected device.	9.8	More Details
CVE-2023-0839	Improper Protection for Outbound Error Messages and Alert Signals vulnerability in ProMIS Process Co. InSCADA allows Account Footprinting.This issue affects inSCADA: before 20230115-1.	9.8	More Details
CVE-2022-4328	The WooCommerce Checkout Field Manager WordPress plugin before 18.0 does not validate files to be uploaded, which could allow unauthenticated attackers to upload arbitrary files such as PHP on the server	9.8	More Details
CVE-2023-0979	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in MedData MedDataPACS allows SQL Injection.This issue affects MedDataPACS : before 2023-03-03.	9.8	More Details
CVE-2023-24776	Funadmin v3.2.0 was discovered to contain a remote code execution (RCE) vulnerability via the component \controller\Addon.php.	9.8	More Details
CVE-2021-36392	In Moodle, an SQL injection risk was identified in the library fetching a user's enrolled courses.	9.8	More Details
CVE-2021-36393	In Moodle, an SQL injection risk was identified in the library fetching a user's recent courses.	9.8	More Details
CVE-2021-36394	In Moodle, a remote code execution risk was identified in the Shibboleth authentication plugin.	9.8	More Details
CVE-2023-24734	An arbitrary file upload vulnerability in the camera_upload.php component of PMB v7.4.6 allows attackers to execute arbitrary code via a crafted image file.	9.8	More Details
CVE-2023-24736	PMB v7.4.6 was discovered to contain a remote code execution (RCE) vulnerability via the component /sauvegarde/restaure_act.php.	9.8	More Details
CVE-2023-26949	An arbitrary file upload vulnerability in the component /admin1/config/update of onekeyadmin v1.3.9 allows attackers to execute arbitrary code via a crafted PHP file.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45141	Since the Windows Kerberos RC4-HMAC Elevation of Privilege Vulnerability was disclosed by Microsoft on Nov 8 2022 and per RFC8429 it is assumed that rc4-hmac is weak, Vulnerable Samba Active Directory DCs will issue rc4-hmac encrypted tickets despite the target server supporting better encryption (eg aes256-cts-hmac-sha1-96).	9.8	More Details
CVE-2022-3760	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Mia Technology Mia-Med.This issue affects Mia-Med: before 1.0.0.58.	9.8	More Details
CVE-2023-24781	Funadmin v3.2.0 was discovered to contain a SQL injection vulnerability via the selectFields parameter at \member\MemberLevel.php.	9.8	More Details
CVE-2023-25690	Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P] ProxyPassReverse /here/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.	9.8	More Details
CVE-2023-24775	Funadmin v3.2.0 was discovered to contain a SQL injection vulnerability via the selectFields parameter at \member\Member.php.	9.8	More Details
CVE-2022-46973	Report v0.9.8.6 was discovered to contain a Server-Side Request Forgery (SSRF) vulnerability.	9.8	More Details
CVE-2022-37936	Unauthenticated Java deserialization vulnerability in Serviceguard Manager	9.8	More Details
CVE-2023-24642	Judging Management System v1.0 was discovered to contain a SQL injection vulnerability via the sid parameter at /php-jms/updateTxtview.php.	9.8	More Details
CVE-2023-24641	Judging Management System v1.0 was discovered to contain a SQL injection vulnerability via the sid parameter at /php-jms/updateview.php.	9.8	More Details
CVE-2022-37938	Unauthenticated server side request forgery in HPE Serviceguard Manager	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20032	On Feb 15, 2023, the following vulnerability in the ClamAV scanning library was disclosed: A vulnerability in the HFS+ partition file parser of ClamAV versions 1.0.0 and earlier, 0.105.1 and earlier, and 0.103.7 and earlier could allow an unauthenticated, remote attacker to execute arbitrary code. This vulnerability is due to a missing buffer size check that may result in a heap buffer overflow write. An attacker could exploit this vulnerability by submitting a crafted HFS+ partition file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the ClamAV scanning process, or else crash the process, resulting in a denial of service (DoS) condition. For a description of this vulnerability, see the ClamAV blog ["https://blog.clamav.net/"].	9.8	More Details
CVE-2023-22747	There are multiple command injection vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2023-22748	There are multiple command injection vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2023-22749	There are multiple command injection vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2023-22750	There are multiple command injection vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2023-22751	There are stack-based buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2023-22752	There are stack-based buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2023-1064	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Uzay Baskul Weighbridge Automation Software allows SQL Injection.This issue affects Weighbridge Automation Software: before 1.1.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1114	Missing Authorization vulnerability in Eskom e-Belediye allows Information Elicitation.This issue affects e-Belediye: from 1.0.0.95 before 1.0.0.100.	9.8	More Details
CVE-2023-23315	The PrestaShop e-commerce platform module stripejs contains a Blind SQL injection vulnerability up to version 4.5.5. The method `stripejsValidationModuleFrontController::initContent()` has sensitive SQL calls that can be executed with a trivial http call and exploited to forge a SQL injection.	9.8	More Details
CVE-2021-3854	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Glox Technology Useroam Hotspot allows SQL Injection. This issue affects Useroam Hotspot: before 5.1.0.15.	9.8	More Details
CVE-2023-26780	CleverStupidDog yf-exam v 1.8.0 is vulnerable to SQL Injection.	9.8	More Details
CVE-2022-46501	Accruent LLC Maintenance Connection 2021 (all) & 2022.2 was discovered to contain a SQL injection vulnerability via the E-Mail to Work Order function.	9.8	More Details
CVE-2022-45551	An issue discovered in Shenzhen Zhiboton Electronics ZBT WE1626 Router v 21.06.18 allows attackers to escalate privileges via WGET command to the Network Diagnosis endpoint.	9.8	More Details
CVE-2022-45553	An issue discovered in Shenzhen Zhibotong Electronics WBT WE1626 Router v 21.06.18 allows attacker to execute arbitrary commands via serial connection to the UART port.	9.8	More Details
CVE-2023-20078	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory.	9.8	More Details
CVE-2022-37937	Pre-auth memory corruption in HPE Serviceguard	9.8	More Details
CVE-2023-20079	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory.	9.8	More Details
CVE-2023-1097	Baicells EG7035-M11 devices with firmware through BCE-ODU-1.0.8 are vulnerable to improper code exploitation via HTTP GET command injections. Commands are executed using pre-login execution and executed with root permissions. The following methods have been tested and validated by a 3rd party analyst and have been confirmed exploitable special thanks to Lionel Musonza for the discovery.	9.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26481	authentik is an open-source Identity Provider. Due to an insufficient access check, a recovery flow link that is created by an admin (or sent via email by an admin) can be used to set the password for any arbitrary user. This attack is only possible if a recovery flow exists, which has both an Identification and an Email stage bound to it. If the flow has policies on the identification stage to skip it when the flow is restored (by checking `request.context['is_restored']`), the flow is not affected by this. With this flow in place, an administrator must create a recovery Link or send a recovery URL to the attacker, who can, due to the improper validation of the token create, set the password for any account. Regardless, for custom recovery flows it is recommended to add a policy that checks if the flow is restored, and skips the identification stage. This issue has been fixed in versions 2023.2.3, 2023.1.3 and 2022.12.2.	9.1	More Details
CVE-2023-27290	Docker based datastores for IBM Instana (IBM Observability with Instana 239-0 through 239-2, 241-0 through 241-2, and 243-0) do not currently require authentication. Due to this, an attacker within the network could access the datastores with read/write access. IBM X-Force ID: 248737.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-26480	XWiki Platform is a generic wiki platform. Starting in version 12.10, a user without script rights can introduce a stored cross-site scripting by using the Live Data macro. This has been patched in XWiki 14.9, 14.4.7, and 13.10.10. There are no known workarounds.	8.9	More Details
CVE-2023-23929	vantage6 is a privacy preserving federated learning infrastructure for secure insight exchange. Currently, the refresh token is valid indefinitely. The refresh token should get a validity of 24-48 hours. A fix was released in version 3.8.0.	8.8	More Details
CVE-2023-0093	Okta Advanced Server Access Client versions 1.13.1 through 1.65.0 are vulnerable to command injection due to the third party library webbrowser. An outdated library, webbrowser, used by the ASA client was found to be vulnerable to command injection. To exploit this issue, an attacker would need to phish the user to enter an attacker controlled server URL during enrollment.	8.8	More Details
CVE-2023-27475	Goutil is a collection of miscellaneous functionality for the go language. In versions prior to 0.6.0 when users use fsutil.Unzip to unzip zip files from a malicious attacker, they may be vulnerable to path traversal. This vulnerability is known as a ZipSlip. This issue has been fixed in version 0.6.0, users are advised to upgrade. There are no known workarounds for this issue.	8.8	More Details
CVE-2021-4331	The Plus Addons for Elementor plugin for WordPress is vulnerable to privilege escalation in versions up to, and including 4.1.9 (pro) and 2.0.6 (free). The plugin adds a registration form to the Elementor page builders functionality. As part of the registration form, users can choose which role to set as the default for users upon registration. This field is not hidden for lower-level users so any user with access to the Elementor page builder, such as contributors, can set the default role to administrator. Since contributors can not publish posts, only author+ users can elevate privileges without interaction via a site administrator (to approve a post).	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4330	The Envato Elements & Download and Template Kit – Import plugins for WordPress are vulnerable to arbitrary file uploads due to insufficient validation of file type upon extracting uploaded Zip files in the installFreeTemplateKit and uploadTemplateKitZipFile functions. This makes it possible for attackers with contributor-lever permissions and above to upload arbitrary files and potentially gain remote code execution in versions up to and including 1.0.13 of Template Kit – Import and versions up to and including 2.0.10 of Envato Elements & Download.	8.8	More Details
CVE-2023-25222	A heap-based buffer overflow vulnerability exits in GNU LibreDWG v0.12.5 via the bit_read_RC function at bits.c.	8.8	More Details
CVE-2020-36669	The JetBackup – WP Backup, Migrate & Restore plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including 1.3.9. This is due to missing nonce validation on the backup_guard_get_import_backup() function. This makes it possible for unauthenticated attackers to upload arbitrary files to the vulnerable site's server via a forged request, granted they can trick a site's administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2022-45608	An issue was discovered in ThingsBoard 3.4.1, allows low privileged attackers (CUSTOMER_USER) to gain escalated privileges (vertically) and become an Administrator (TENANT_ADMIN) or (SYS_ADMIN) on the web application. It is important to note that in order to accomplish this, the attacker must know the corresponding API's parameter (authority : value).	8.8	More Details
CVE-2023-23554	Uncontrolled search path element vulnerability exists in pg_ivm versions prior to 1.5.1. When refreshing an IMMV, pg_ivm executes functions without specifying schema names. Under certain conditions, pg_ivm may be tricked to execute unexpected functions from other schemas with the IMMV owner's privilege. If this vulnerability is exploited, an unexpected function provided by an attacker may be executed with the privilege of the materialized view owner.	8.8	More Details
CVE-2023-24217	AgileBio Electronic Lab Notebook v4.234 was discovered to contain a local file inclusion vulnerability.	8.8	More Details
CVE-2023-0228	Improper Authentication vulnerability in ABB Symphony Plus S+ Operations.This issue affects Symphony Plus S+ Operations: from 2.X through 2.1 SP2, 2.2, from 3.X through 3.3 SP1, 3.3 SP2.	8.8	More Details
CVE-2023-24763	In the module "Xen Forum" (xenforum) for PrestaShop, an authenticated user can perform SQL injection in versions up to 2.13.0.	8.8	More Details
CVE-2023-0951	Improper access controls on some API endpoints in Devolutions Server 2022.3.12 and earlier could allow a standard privileged user to perform privileged actions.	8.8	More Details
CVE-2023-25358	A use-after-free vulnerability in WebCore::RenderLayer::addChild in WebKitGTK before 2.36.8 allows attackers to execute code remotely.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25360	A use-after-free vulnerability in WebCore::RenderLayer::renderer in WebKitGTK before 2.36.8 allows attackers to execute code remotely.	8.8	More Details
CVE-2023-25361	A use-after-free vulnerability in WebCore::RenderLayer::setNextSibling in WebKitGTK before 2.36.8 allows attackers to execute code remotely.	8.8	More Details
CVE-2023-25362	A use-after-free vulnerability in WebCore::RenderLayer::repaintBlockSelectionGaps in WebKitGTK before 2.36.8 allows attackers to execute code remotely.	8.8	More Details
CVE-2023-25363	A use-after-free vulnerability in WebCore::RenderLayer::updateDescendantDependentFlags in WebKitGTK before 2.36.8 allows attackers to execute code remotely.	8.8	More Details
CVE-2023-24789	jeecg-boot v3.4.4 was discovered to contain an authenticated SQL injection vulnerability via the building block report component.	8.8	More Details
CVE-2022-4265	The Replyable WordPress plugin before 2.2.10 does not validate the class name submitted by the request when instantiating an object in the prompt_dismiss_notice action and also lacks CSRF check in the related action. This could allow any authenticated users, such as subscriber to perform Object Injection attacks. The attack could also be done via a CSRF vector against any authenticated user	8.8	More Details
CVE-2022-46395	An issue was discovered in the Arm Mali GPU Kernel Driver. A non-privileged user can make improper GPU processing operations to gain access to already freed memory. This affects Midgard r0p0 through r32p0, Bifrost r0p0 through r41p0 before r42p0, Valhall r19p0 through r41p0 before r42p0, and Avalon r41p0 before r42p0.	8.8	More Details
CVE-2023-1101	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes.	8.8	More Details
CVE-2023-0953	Insufficient input sanitization in the documentation feature of Devolutions Server 2022.3.12 and earlier allows an authenticated attacker to perform an SQL Injection, potentially resulting in unauthorized access to system resources.	8.8	More Details
CVE-2019-8720	A vulnerability was found in WebKit. The flaw is triggered when processing maliciously crafted web content that may lead to arbitrary code execution. Improved memory handling addresses the multiple memory corruption issues.	8.8	More Details
CVE-2023-1222	Heap buffer overflow in Web Audio API in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-1215	Type confusion in CSS in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1213	Use after free in Swiftshader in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-1227	Use after free in Core in Google Chrome on Lacros prior to 111.0.5563.64 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via crafted UI interaction. (Chromium security severity: Medium)	8.8	More Details
CVE-2021-3855	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in Liman Central Management System Liman MYS (HTTP/Controllers, CronMail, Jobs modules) allows Command Injection.This issue affects Liman Central Management System: from 1.7.0 before 1.8.3-462.	8.8	More Details
CVE-2023-1220	Heap buffer overflow in UMA in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-1214	Type confusion in V8 in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-1219	Heap buffer overflow in Metrics in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-1218	Use after free in WebRTC in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-1216	Use after free in DevTools in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had convienced the user to engage in direct UI interaction to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-4904	A flaw was found in the c-ares package. The ares_set_sortlist is missing checks about the validity of the input string, which allows a possible arbitrary length stack overflow. This issue may cause a denial of service or a limited impact on confidentiality and integrity.	8.6	More Details
CVE-2023-22856	A stored Cross-site Scripting (XSS) vulnerability in BlogEngine.NET 3.3.8.0, allows injection of arbitrary JavaScript in the security context of a blog visitor through an upload of a specially crafted file.	8.5	More Details
CVE-2023-22857	A stored Cross-site Scripting (XSS) vulnerability in BlogEngine.NET 3.3.8.0, allows injection of arbitrary JavaScript in the security context of a blog visitor through an injection of a malicious payload into a blog post.	8.5	More Details
CVE-2023-1164	A vulnerability was found in KylinSoft kylin-activation on KylinOS and classified as critical. Affected by this issue is some unknown functionality of the component File Import. The manipulation leads to improper authorization. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. Upgrading to version 1.3.11-23 and 1.30.10-5.p23 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-222260.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0957	An issue was discovered in Gitpod versions prior to release-2022.11.2.16. There is a Cross-Site WebSocket Hijacking (CSWSH) vulnerability that allows attackers to make WebSocket connections to the Gitpod JSONRPC server using a victim's credentials, because the Origin header is not restricted. This can lead to the extraction of data from workspaces, to a full takeover of the workspace.	8.2	More Details
CVE-2023-27472	quickentity-editor-next is an open source, system local, video game asset editor. In affected versions HTML tags in entity names are not sanitised (XSS vulnerability). Allows arbitrary code execution within the browser sandbox, among other things, simply from loading a file containing a script tag in any entity name. This issue has been patched in version 1.28.1 of the application. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.2	More Details
CVE-2022-42476	A relative path traversal vulnerability [CWE-23] in Fortinet FortiOS version 7.2.0 through 7.2.2, 7.0.0 through 7.0.8 and before 6.4.11, FortiProxy version 7.2.0 through 7.2.2 and 7.0.0 through 7.0.8 allows privileged VDOM administrators to escalate their privileges to super admin of the box via crafted CLI requests.	8.2	More Details
CVE-2023-1105	External Control of File Name or Path in GitHub repository flatpressblog/flatpress prior to 1.3.	8.1	More Details
CVE-2023-22757	There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	8.1	More Details
CVE-2023-22756	There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	8.1	More Details
CVE-2023-22755	There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	8.1	More Details
CVE-2023-22754	There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	8.1	More Details
CVE-2023-22753	There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27474	Directus is a real-time API and App dashboard for managing SQL database content. Instances relying on an allow-listed reset URL are vulnerable to an HTML injection attack through the use of query parameters in the reset URL. An attacker could exploit this to email users urls to the servers domain but which may contain malicious code. The problem has been resolved and released under version 9.23.0. People relying on a custom password reset URL should upgrade to 9.23.0 or later, or remove the custom reset url from the configured allow list. Users are advised to upgrade. Users unable to upgrade may disable the custom reset URL allow list as a workaround.	8.0	More Details
CVE-2023-1127	Divide By Zero in GitHub repository vim/vim prior to 9.0.1367.	7.8	More Details
CVE-2023-1118	A flaw use after free in the Linux kernel integrated infrared receiver/transceiver driver was found in the way user detaching rc device. A local user could use this flaw to crash the system or potentially escalate their privileges on the system.	7.8	More Details
CVE-2023-22424	Use-after-free vulnerability exists in Kostac PLC Programming Software (Former name: Koyo PLC Programming Software) Version 1.6.9.0 and earlier. With the abnormal value given as the maximum number of columns for the PLC program, the process accesses the freed memory. As a result, opening a specially crafted project file may lead to information disclosure and/or arbitrary code execution.	7.8	More Details
CVE-2023-25221	Libde265 v1.0.10 was discovered to contain a heap-buffer-overflow vulnerability in the derive_spatial_luma_vector_prediction function in motion.cc.	7.8	More Details
CVE-2023-25304	An issue in Prism Launcher up to v6.1 allows attackers to perform a directory traversal via importing a crafted .mrpack file.	7.8	More Details
CVE-2022-39953	A improper privilege management in Fortinet FortiNAC version 9.4.0 through 9.4.1, FortiNAC version 9.2.0 through 9.2.6, FortiNAC version 9.1.0 through 9.1.8, FortiNAC all versions 8.8, FortiNAC all versions 8.7, FortiNAC all versions 8.6, FortiNAC all versions 8.5, FortiNAC version 8.3.7 allows attacker to escalation of privilege via specially crafted commands.	7.8	More Details
CVE-2022-3424	A use-after-free flaw was found in the Linux kernel's SGI GRU driver in the way the first gru_file_unlocked_ioctl function is called by the user, where a fail pass occurs in the gru_check_chiplet_assignment function. This flaw allows a local user to crash or potentially escalate their privileges on the system.	7.8	More Details
CVE-2022-27677	Failure to validate privileges during installation of AMD Ryzen™ Master may allow an attacker with low privileges to modify files potentially leading to privilege escalation and code execution by the lower privileged user.	7.8	More Details
CVE-2022-45988	starsoftcomm CooCare 5.304 allows local attackers to escalate privileges and execute arbitrary commands via a crafted file upload.	7.8	More Details
CVE-2022-47664	Libde265 1.0.9 is vulnerable to Buffer Overflow in ff_hevc_put_hevc_qpel_pixels_8_sse	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47665	Libde265 1.0.9 has a heap buffer overflow vulnerability in de265_image::set_SliceAddrRS(int, int, int)	7.8	More Details
CVE-2023-27566	Cubism Core in Live2D Cubism Editor 4.2.03 allows out-of-bounds write via a crafted Section Offset Table or Count Info Table in an MOC3 file.	7.8	More Details
CVE-2023-22421	Out-of-bounds read vulnerability exists in Kostac PLC Programming Software (Former name: Koyo PLC Programming Software) Version 1.6.9.0 and earlier. The insufficient buffer size for the PLC program instructions leads to out-of-bounds read. As a result, opening a specially crafted project file may lead to information disclosure and/or arbitrary code execution.	7.8	More Details
CVE-2023-22419	Out-of-bounds read vulnerability exists in Kostac PLC Programming Software (Former name: Koyo PLC Programming Software) Version 1.6.9.0 and earlier. When processing a comment block in stage information, the end of data cannot be verified and out-of-bounds read occurs. As a result, opening a specially crafted project file may lead to information disclosure and/or arbitrary code execution.	7.8	More Details
CVE-2023-26604	systemd before 247 does not adequately block local privilege escalation for some Sudo configurations, e.g., plausible sudoers files in which the "systemctl status" command may be executed. Specifically, systemd does not set LESSSECURE to 1, and thus other programs may be launched from the less program. This presents a substantial security risk when running systemctl from Sudo, because less executes as root when the terminal size is too small to show the complete systemctl output.	7.8	More Details
CVE-2023-27635	debmany in debian-goodies 0.88.1 allows attackers to execute arbitrary shell commands (because of an eval call) via a crafted .deb file. (The path is shown to the user before execution.)	7.8	More Details
CVE-2023-27480	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions any user with edit rights on a document can trigger an XAR import on a forged XAR file, leading to the ability to display the content of any file on the XWiki server host. This vulnerability has been patched in XWiki 13.10.11, 14.4.7 and 14.10-rc-1. Users are advised to upgrade. Users unable to upgrade may apply the patch `e3527b98fd` manually.	7.7	More Details
CVE-2023-0567	In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, password_verify() function may accept some invalid Blowfish hashes as valid. If such invalid hash ever ends up in the password database, it may lead to an application allowing any password for this entry as valid.	7.7	More Details
CVE-2023-1257	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device’s authentication files to create a new user and gain full access to the system.	7.6	More Details
CVE-2023-25402	CleverStupidDog yf-exam 1.8.0 is vulnerable to File Upload. There is no restriction on the suffix of the uploaded file, resulting in any file upload.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25403	CleverStupidDog yf-exam v 1.8.0 is vulnerable to Authentication Bypass. The program uses a fixed JWT key, and the stored key uses username format characters. Any user who logged in within 24 hours. A token can be forged with his username to bypass authentication.	7.5	More Details
CVE-2023-26601	Zoho ManageEngine ServiceDesk Plus through 14104, Asset Explorer through 6987, ServiceDesk Plus MSP before 14000, and Support Center Plus before 14000 allow Denial-of-Service (DoS).	7.5	More Details
CVE-2023-20014	A vulnerability in the DNS functionality of Cisco Nexus Dashboard Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. This vulnerability is due to the improper processing of DNS requests. An attacker could exploit this vulnerability by sending a continuous stream of DNS requests to an affected device. A successful exploit could allow the attacker to cause the coredns service to stop working or cause the device to reload, resulting in a DoS condition.	7.5	More Details
CVE-2023-24567	Dell NetWorker versions 19.5 and earlier contain 'RabbitMQ' version disclosure vulnerability. A NetWorker server user with remote access to NetWorker clients may potentially exploit this vulnerability and may launch target-specific attacks.	7.5	More Details
CVE-2023-27567	In OpenBSD 7.2, a TCP packet with destination port 0 that matches a pf divert-to rule can crash the kernel.	7.5	More Details
CVE-2021-36395	In Moodle, the file repository's URL parsing required additional recursion handling to mitigate the risk of recursion denial of service.	7.5	More Details
CVE-2023-22335	Improper access control vulnerability in SS1 Ver.13.0.0.40 and earlier and Rakuraku PC Cloud Agent Ver.2.1.8 and earlier allows a remote attacker to bypass access restriction and download an arbitrary file of the directory where the product runs. As a result of exploiting this vulnerability with CVE-2023-22336 and CVE-2023-22344 vulnerabilities together, it may allow a remote attacker to execute an arbitrary code with SYSTEM privileges by sending a specially crafted script to the affected device.	7.5	More Details
CVE-2021-36396	In Moodle, insufficient redirect handling made it possible to blindly bypass cURL blocked hosts/allowed ports restrictions, resulting in a blind SSRF risk.	7.5	More Details
CVE-2022-45142	The fix for CVE-2022-3437 included changing memcmp to be constant time and a workaround for a compiler bug by adding "!= 0" comparisons to the result of memcmp. When these patches were backported to the heimdal-7.7.1 and heimdal-7.8.0 branches (and possibly other branches) a logic inversion sneaked in causing the validation of message integrity codes in gssapi/arcfour to be inverted.	7.5	More Details
CVE-2023-27891	rami.io pretix before 4.17.1 allows OAuth application authorization from a logged-out session. The fixed versions are 4.15.1, 4.16.1, and 4.17.1.	7.5	More Details
CVE-2022-38734	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.6.0.8 are susceptible to a Denial of Service (DoS) vulnerability. A successful exploit could lead to to a crash of the Local Distribution Router (LDR) service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25544	Dell NetWorker versions 19.5 and earlier contain 'Apache Tomcat' version disclosure vulnerability. A NetWorker server user with remote access to NetWorker clients may potentially exploit this vulnerability and may launch target-specific attacks.	7.5	More Details
CVE-2023-26476	XWiki Platform is a generic wiki platform. Starting in version 3.2-m3, users can deduce the content of the password fields by repeated call to `LiveTableResults` and `WikisLiveTableResultsMacros`. The issue can be fixed by upgrading to versions 14.7-rc-1, 13.4.4, or 13.10.9 and higher, or in version >= 3.2M3 by applying the patch manually on `LiveTableResults` and `WikisLiveTableResultsMacros`.	7.5	More Details
CVE-2023-0656	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash.	7.5	More Details
CVE-2023-0457	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series, MELSEC iQ-R Series, MELSEC-Q Series and MELSEC-L Series allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server.	7.5	More Details
CVE-2023-0053	SAUTER Controls Nova 200–220 Series with firmware version 3.3-006 and prior and BACnetstac version 4.2.1 and prior have only FTP and Telnet available for device management. Any sensitive information communicated through these protocols, such as credentials, is sent in cleartext. An attacker could obtain sensitive information such as user credentials to gain access to the system.	7.5	More Details
CVE-2023-27560	Math/PrimeField.php in phpseclib 3.x before 3.0.19 has an infinite loop with composite primefields.	7.5	More Details
CVE-2022-45552	An Insecure Permissions vulnerability in Shenzhen Zhiboton Electronics ZBT WE1626 Router v 21.06.18 allows attackers to obtain sensitive information via SPI bus interface connected to pinout of the NAND flash memory.	7.5	More Details
CVE-2022-41333	An uncontrolled resource consumption vulnerability [CWE-400] in FortiRecorder version 6.4.3 and below, 6.0.11 and below login authentication mechanism may allow an unauthenticated attacker to make the device unavailable via crafted GET requests.	7.5	More Details
CVE-2023-25605	A improper access control vulnerability in Fortinet FortiSOAR 7.3.0 - 7.3.1 allows an attacker authenticated on the administrative interface to perform unauthorized actions via crafted HTTP requests.	7.5	More Details
CVE-2023-26106	All versions of the package dot-lens are vulnerable to Prototype Pollution via the set() function in index.js file.	7.5	More Details
CVE-2023-27522	HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55. Special characters in the origin response header can truncate/split the response forwarded to the client.	7.5	More Details
CVE-2023-26111	All versions of the package @nubosoftware/node-static; all versions of the package node-static are vulnerable to Directory Traversal due to improper file path sanitization in the startsWith() method in the servePath function.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40676	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiNAC versions 9.4.0, 9.2.0 through 9.2.5, 9.1.0 through 9.1.8, 8.8.0 through 8.8.11, 8.7.0 through 8.7.6, 8.6.0 through 8.6.5, 8.5.0 through 8.5.4, 8.3.7 allows attacker to execute unauthorized code or commands via specially crafted http requests.	7.5	More Details
CVE-2023-26490	mailcow is a dockerized email package, with multiple containers linked in one bridged network. The Sync Job feature - which can be made available to standard users by assigning them the necessary permission - suffers from a shell command injection. A malicious user can abuse this vulnerability to obtain shell access to the Docker container running dovecot. The imapsync Perl script implements all the necessary functionality for this feature, including the XOAUTH2 authentication mechanism. This code path creates a shell command to call openssl. However, since different parts of the specified user password are included without any validation, one can simply execute additional shell commands. Notably, the default ACL for a newly-created mailcow account does not include the necessary permission. The Issue has been fixed within the 2023-03 Update (March 3rd 2023). As a temporary workaround the Syncjob ACL can be removed from all mailbox users, preventing from creating or changing existing Syncjobs.	7.3	More Details
CVE-2023-1253	A vulnerability, which was classified as critical, was found in SourceCodester Health Center Patient Record Management System 1.0. This affects an unknown part of the file 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 associated identifier of this vulnerability is VDB-222483.	7.3	More Details
CVE-2023-0507	Grafana is an open-source platform for monitoring and observability. Starting with the 8.1 branch, Grafana had a stored XSS vulnerability affecting the core plugin GeoMap. The stored XSS vulnerability was possible due to map attributions weren't properly sanitized and allowed arbitrary JavaScript to be executed in the context of the currently authorized user of the Grafana instance. An attacker needs to have the Editor role in order to change a panel to include a map attribution containing JavaScript. This means that vertical privilege escalation is possible, where a user with Editor role can change to a known password for a user having Admin role if the user with Admin role executes malicious JavaScript viewing a dashboard. Users may upgrade to version 8.5.21, 9.2.13 and 9.3.8 to receive a fix.	7.3	More Details
CVE-2023-0594	Grafana is an open-source platform for monitoring and observability. Starting with the 7.0 branch, Grafana had a stored XSS vulnerability in the trace view visualization. The stored XSS vulnerability was possible due the value of a span's attributes/resources were not properly sanitized and this will be rendered when the span's attributes/resources are expanded. An attacker needs to have the Editor role in order to change the value of a trace view visualization to contain JavaScript. This means that vertical privilege escalation is possible, where a user with Editor role can change to a known password for a user having Admin role if the user with Admin role executes malicious JavaScript viewing a dashboard. Users may upgrade to version 8.5.21, 9.2.13 and 9.3.8 to receive a fix.	7.3	More Details
CVE-2023-22773	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system.	7.2	More Details
CVE-2023-22770	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22768	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2023-25223	CRMEB <=1.3.4 is vulnerable to SQL Injection via /api/admin/user/list.	7.2	More Details
CVE-2023-1162	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in DrayTek Vigor 2960 1.5.1.4/1.5.1.5. Affected is an unknown function of the file mainfunction.cgi of the component Web Management Interface. The manipulation of the argument password leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-222258 is the identifier assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	7.2	More Details
CVE-2023-26213	On Barracuda CloudGen WAN Private Edge Gateway devices before 8 webui-sdwan-1089-8.3.1-174141891, an OS command injection vulnerability exists in /ajax/update_certificate - a crafted HTTP request allows an authenticated attacker to execute arbitrary commands. For example, a name field can contain :password and a password field can contain shell metacharacters.	7.2	More Details
CVE-2023-22758	Authenticated remote command injection vulnerabilities exist in the ArubaOS web-based management interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS.	7.2	More Details
CVE-2023-22759	Authenticated remote command injection vulnerabilities exist in the ArubaOS web-based management interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS.	7.2	More Details
CVE-2023-22769	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2022-39951	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWeb version 7.0.0 through 7.0.2, FortiWeb version 6.3.6 through 6.3.20, FortiWeb 6.4 all versions allows attacker to execute unauthorized code or commands via specifically crafted HTTP requests.	7.2	More Details
CVE-2023-22767	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2023-22766	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22765	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2023-22774	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system.	7.2	More Details
CVE-2023-0084	The Metform Elementor Contact Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via text areas on forms in versions up to, and including, 3.1.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page, which is the submissions page.	7.2	More Details
CVE-2023-22763	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2023-22762	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2023-22761	Authenticated remote command injection vulnerabilities exist in the ArubaOS web-based management interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS.	7.2	More Details
CVE-2023-1211	SQL Injection in GitHub repository phpipam/phpipam prior to v1.5.2.	7.2	More Details
CVE-2023-22760	Authenticated remote command injection vulnerabilities exist in the ArubaOS web-based management interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS.	7.2	More Details
CVE-2023-22764	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2023-27561	runc through 1.1.4 has Incorrect Access Control leading to Escalation of Privileges, related to libcontainer/rootfs_linux.go. To exploit this, an attacker must be able to spawn two containers with custom volume-mount configurations, and be able to run custom images. NOTE: this issue exists because of a CVE-2019-19921 regression.	7.0	More Details
CVE-2023-26107	All versions of the package sketchsvg are vulnerable to Arbitrary Code Injection when invoking shell.exec without sanitization nor parametrization while concatenating the current directory as part of the command string.	6.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22771	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on an affected device after the removal of the impacted account	6.8	More Details
CVE-2022-4645	LibTIFF 4.4.0 has an out-of-bounds read in tiffcp in tools/tiffcp.c:948, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit e8131125.	6.8	More Details
CVE-2023-20636	In display drm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07292593; Issue ID: ALPS07292593.	6.7	More Details
CVE-2023-25536	Dell PowerScale OneFS 9.4.0.x contains exposure of sensitive information to an unauthorized actor. A malicious authenticated local user could potentially exploit this vulnerability in certificate management, leading to a potential system takeover.	6.7	More Details
CVE-2023-20637	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628588; Issue ID: ALPS07628588.	6.7	More Details
CVE-2022-41328	A improper limitation of a pathname to a restricted directory vulnerability ('path traversal') [CWE-22] in Fortinet FortiOS version 7.2.0 through 7.2.3, 7.0.0 through 7.0.9 and before 6.4.11 allows a privileged attacker to read and write files on the underlying Linux system via crafted CLI commands.	6.7	More Details
CVE-2023-20640	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629573; Issue ID: ALPS07629573.	6.7	More Details
CVE-2023-20642	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628586; Issue ID: ALPS07628586.	6.7	More Details
CVE-2023-20633	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508.	6.7	More Details
CVE-2023-20632	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506.	6.7	More Details
CVE-2023-20641	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629574; Issue ID: ALPS07629574.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20638	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537.	6.7	More Details
CVE-2023-20630	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505.	6.7	More Details
CVE-2023-20643	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584.	6.7	More Details
CVE-2023-20634	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697.	6.7	More Details
CVE-2023-20639	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628587; Issue ID: ALPS07628587.	6.7	More Details
CVE-2023-20621	In tinysys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664755; Issue ID: ALPS07664755.	6.7	More Details
CVE-2023-20650	In apu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629577; Issue ID: ALPS07629577.	6.7	More Details
CVE-2023-20624	In vow, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628530; Issue ID: ALPS07628530.	6.7	More Details
CVE-2023-20626	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223.	6.7	More Details
CVE-2023-20627	In pqframework, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629585; Issue ID: ALPS07629585.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20628	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460.	6.7	More Details
CVE-2023-26478	XWiki Platform is a generic wiki platform. Starting in version 14.3-rc-1, `org.xwiki.store.script.TemporaryAttachmentsScriptService#uploadTemporaryAttachment` returns an instance of `com.xpn.xwiki.doc.XWikiAttachment`. This class is not supported to be exposed to users without the `programing` right. `com.xpn.xwiki.api.Attachment` should be used instead and takes case of checking the user's rights before performing dangerous operations. This has been patched in versions 14.9-rc-1 and 14.4.6. There are no known workarounds for this issue.	6.6	More Details
CVE-2023-26053	Gradle is a build tool with a focus on build automation and support for multi-language development. This is a collision attack on long IDs (64bits) for PGP keys. Users of dependency verification in Gradle are vulnerable if they use long IDs for PGP keys in a `trusted-key` or `pgp` element in their dependency verification metadata file. The fix is to fail dependency verification if anything but a fingerprint is used in a trust element in dependency verification metadata. The problem is fixed in Gradle 8.0 and above. The problem is also patched in Gradle 6.9.4 and 7.6.1. As a workaround, use only full fingerprint IDs for `trusted-key` or `pgp` element in the metadata is a protection against this issue.	6.6	More Details
CVE-2022-3294	Users may have access to secure endpoints in the control plane network. Kubernetes clusters are only affected if an untrusted user can modify Node objects and send proxy requests to them. Kubernetes supports node proxying, which allows clients of kube-apiserver to access endpoints of a Kubelet to establish connections to Pods, retrieve container logs, and more. While Kubernetes already validates the proxying address for Nodes, a bug in kube-apiserver made it possible to bypass this validation. Bypassing this validation could allow authenticated requests destined for Nodes to to the API server's private network.	6.6	More Details
CVE-2023-1170	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.1376.	6.6	More Details
CVE-2023-1175	Incorrect Calculation of Buffer Size in GitHub repository vim/vim prior to 9.0.1378.	6.6	More Details
CVE-2023-26051	Saleor is a headless, GraphQL commerce platform delivering personalized shopping experiences. Some internal Python exceptions are not handled properly and thus are returned in API as error messages. Some messages might contain sensitive information like user email address in staff-authenticated requests.	6.5	More Details
CVE-2023-24118	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the security parameter at /goform/WifiBasicSet.	6.5	More Details
CVE-2023-1226	Insufficient policy enforcement in Web Payments API in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26473	XWiki Platform is a generic wiki platform. Starting in version 1.3-rc-1, any user with edit right can execute arbitrary database select and access data stored in the database. The problem has been patched in XWiki 13.10.11, 14.4.7, and 14.10. There is no workaround for this vulnerability other than upgrading.	6.5	More Details
CVE-2023-26479	XWiki Platform is a generic wiki platform. Starting in version 6.0, users with write rights can insert well-formed content that is not handled well by the parser. As a consequence, some pages becomes unusable, including the user index (if the page containing the faulty content is a user page) and the page index. Note that on the page, the normal UI is completely missing and it is not possible to open the editor directly to revert the change as the stack overflow is already triggered while getting the title of the document. This means that it is quite difficult to remove this content once inserted. This has been patched in XWiki 13.10.10, 14.4.6, and 14.9-rc-1. A temporary workaround to avoid Stack Overflow errors is to increase the memory allocated to the stack by using the `-Xss` JVM parameter (e.g., `-Xss32m`). This should allow the parser to pass and to fix the faulty content. The consequences for other aspects of the system (e.g., performance) are unknown, and this workaround should be only be used as a temporary solution. The workaround does not prevent the issue occurring again with other content. Consequently, it is strongly advised to upgrade to a version where the issue has been patched.	6.5	More Details
CVE-2023-20009	A vulnerability in the Web UI and administrative CLI of the Cisco Secure Email Gateway (ESA) and Cisco Secure Email and Web Manager (SMA) could allow an authenticated remote attacker and or authenticated local attacker to escalate their privilege level and gain root access. The attacker has to have a valid user credential with at least a [[privilege of operator - validate actual name]]. The vulnerability is due to the processing of a specially crafted SNMP configuration file. An attacker could exploit this vulnerability by authenticating to the targeted device and uploading a specially crafted SNMP configuration file that when uploaded could allow for the execution of commands as root. An exploit could allow the attacker to gain root access on the device.	6.5	More Details
CVE-2023-24117	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepauth_5g parameter at /goform/WifiBasicSet.	6.5	More Details
CVE-2022-3284	Download key for a file in a vault was passed in an insecure way that could easily be logged in M-Files New Web in M-Files before 22.11.12011.0. This issue affects M-Files New Web: before 22.11.12011.0.	6.5	More Details
CVE-2023-24045	In Dataiku DSS 11.2.1, an attacker can download other Dataiku files that were uploaded to the myfiles section by specifying the target username in a download request.	6.5	More Details
CVE-2021-4332	The Plus Addons for Elementor plugin for WordPress is vulnerable to arbitrary file reads in versions up to, and including 4.1.9 (pro) and 2.0.6 (free). The plugin has a feature to add an "Info Box" to an Elementor created page. This Info Box can include an SVG image for the box. Unfortunately, the plugin used file_get_contents with no verification that the file being supplied was an SVG file, so any user with access to the Elementor page builder, such as contributors, could read arbitrary files on the WordPress installation.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4333	The WP Statistics plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 13.1.1. This is due to missing or incorrect nonce validation on the view() function. This makes it possible for unauthenticated attackers to activate and deactivate arbitrary plugins, via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.5	More Details
CVE-2022-45861	An access of uninitialized pointer vulnerability [CWE-824] in the SSL VPN portal of Fortinet FortiOS version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.9 and before 6.4.11 and FortiProxy version 7.2.0 through 7.2.1, version 7.0.0 through 7.0.7 and before 2.0.11 allows a remote authenticated attacker to crash the sslvpn daemon via an HTTP GET request.	6.5	More Details
CVE-2023-1163	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in DrayTek Vigor 2960 1.5.1.4/1.5.1.5 and classified as critical. Affected by this vulnerability is the function getSyslogFile of the file mainfunction.cgi of the component Web Management Interface. The manipulation of the argument option leads to path traversal. 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-222259. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	6.5	More Details
CVE-2023-27478	libmemcached-awesome is an open source C/C++ client library and tools for the memcached server. `libmemcached` could return data for a previously requested key, if that previous request timed out due to a low `POLL_TIMEOUT`. This issue has been addressed in version 1.1.4. Users are advised to upgrade. There are several ways to workaround or lower the probability of this bug affecting a given deployment. 1: use a reasonably high `POLL_TIMEOUT` setting, like the default. 2: use separate libmemcached connections for unrelated data. 3: do not re-use libmemcached connections in an unknown state.	6.5	More Details
CVE-2023-22775	A vulnerability exists which allows an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level.	6.5	More Details
CVE-2023-22772	An authenticated path traversal vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to delete arbitrary files in the underlying operating system.	6.5	More Details
CVE-2023-24751	libde265 v1.0.10 was discovered to contain a NULL pointer dereference in the mc_chroma function at motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input file.	6.5	More Details
CVE-2022-3162	Users authorized to list or watch one type of namespaced custom resource cluster-wide can read custom resources of a different type in the same API group without authorization. Clusters are impacted by this vulnerability if all of the following are true: 1. There are 2+ CustomResourceDefinitions sharing the same API group 2. Users have cluster-wide list or watch authorization on one of those custom resources. 3. The same users are not authorized to read another custom resource in the same API group.	6.5	More Details
CVE-2023-24132	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey3_5g parameter at /goform/WifiBasicSet.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24126	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey4_5g parameter at /goform/WifiBasicSet.	6.5	More Details
CVE-2023-1217	Stack buffer overflow in Crash reporting in Google Chrome on Windows prior to 111.0.5563.64 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2023-24133	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey_5g parameter at /goform/WifiBasicSet.	6.5	More Details
CVE-2023-26046	teler-waf is a Go HTTP middleware that provides teler IDS functionality to protect against web-based attacks. In teler-waf prior to version 0.1.1 is vulnerable to bypassing common web attack rules when a specific HTML entities payload is used. This vulnerability allows an attacker to execute arbitrary JavaScript code on the victim's browser and compromise the security of the web application. The vulnerability exists due to teler-waf failure to properly sanitize and filter HTML entities in user input. An attacker can exploit this vulnerability to bypass common web attack threat rules in teler-waf and launch cross-site scripting (XSS) attacks. The attacker can execute arbitrary JavaScript code on the victim's browser and steal sensitive information, such as login credentials and session tokens, or take control of the victim's browser and perform malicious actions. This issue has been fixed in version 0.1.1.	6.5	More Details
CVE-2023-24134	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey3 parameter at /goform/WifiBasicSet.	6.5	More Details
CVE-2023-26488	OpenZeppelin Contracts is a library for secure smart contract development. The ERC721Consecutive contract designed for minting NFTs in batches does not update balances when a batch has size 1 and consists of a single token. Subsequent transfers from the receiver of that token may overflow the balance as reported by `balanceOf`. The issue exclusively presents with batches of size 1. The issue has been patched in 4.8.2.	6.5	More Details
CVE-2023-24127	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey1 parameter at /goform/WifiBasicSet.	6.5	More Details
CVE-2023-24125	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey2_5g parameter at /goform/WifiBasicSet.	6.5	More Details
CVE-2023-24131	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey1_5g parameter at /goform/WifiBasicSet.	6.5	More Details
CVE-2023-24124	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wrlEn parameter at /goform/WifiBasicSet.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24123	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepauth parameter at /goform/WifiBasicSet.	6.5	More Details
CVE-2023-24122	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the ssid_5g parameter at /goform/WifiBasicSet.	6.5	More Details
CVE-2023-24121	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the security_5g parameter at /goform/WifiBasicSet.	6.5	More Details
CVE-2023-24120	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wrlEn_5g parameter at /goform/WifiBasicSet.	6.5	More Details
CVE-2023-24119	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the ssid parameter at /goform/WifiBasicSet.	6.5	More Details
CVE-2023-20062	Multiple vulnerabilities in Cisco Unified Intelligence Center could allow an authenticated, remote attacker to collect sensitive information or perform a server-side request forgery (SSRF) attack on an affected system. Cisco plans to release software updates that address these vulnerabilities.	6.5	More Details
CVE-2023-20061	Multiple vulnerabilities in Cisco Unified Intelligence Center could allow an authenticated, remote attacker to collect sensitive information or perform a server-side request forgery (SSRF) attack on an affected system. Cisco plans to release software updates that address these vulnerabilities.	6.5	More Details
CVE-2023-26600	ManageEngine ServiceDesk Plus through 14104, ServiceDesk Plus MSP through 14000, Support Center Plus through 14000, and Asset Explorer through 6987 allow privilege escalation via query reports.	6.5	More Details
CVE-2023-26054	BuildKit is a toolkit for converting source code to build artifacts in an efficient, expressive and repeatable manner. In affected versions when the user sends a build request that contains a Git URL that contains credentials and the build creates a provenance attestation describing that build, these credentials could be visible from the provenance attestation. Git URL can be passed in two ways: 1) Invoking build directly from a URL with credentials. 2) If the client sends additional version control system (VCS) info hint parameters on builds from a local source. Usually, that would mean reading the origin URL from `.git/config` file. When a build is performed under specific conditions where credentials were passed to BuildKit they may be visible to everyone who has access to provenance attestation. Provenance attestations and VCS info hints were added in version v0.11.0. Previous versions are not vulnerable. In v0.10, when building directly from Git URL, the same URL could be visible in `BuildInfo` structure that is a predecessor of Provenance attestations. Previous versions are not vulnerable. This bug has been fixed in v0.11.4. Users are advised to upgrade. Users unable to upgrade may disable VCS info hints by setting `BUILDX_GIT_INFO=0`. `buildctl` does not set VCS hints based on `.git` directory, and values would need to be passed manually with `--opt`.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3854	A flaw was found in Ceph, relating to the URL processing on RGW backends. An attacker can exploit the URL processing by providing a null URL to crash the RGW, causing a denial of service.	6.5	More Details
CVE-2023-26487	Vega is a visualization grammar, a declarative format for creating, saving, and sharing interactive visualization designs.`lassoAppend' function accepts 3 arguments and internally invokes `push` function on the 1st argument specifying array consisting of 2nd and 3rd arguments as `push` call argument. The type of the 1st argument is supposed to be an array, but it's not enforced. This makes it possible to specify any object with a `push` function as the 1st argument, `push` function can be set to any function that can be access via `event.view` (no all such functions can be exploited due to invalid context or signature, but some can, e.g. `console.log`). The issue is that`lassoAppend` doesn't enforce proper types of its arguments. This issue opens various XSS vectors, but exact impact and severity depends on the environment (e.g. Core JS `setImmediate` polyfill basically allows `eval`-like functionality). This issue was patched in 5.23.0.	6.5	More Details
CVE-2022-3277	An uncontrolled resource consumption flaw was found in openstack-neutron. This flaw allows a remote authenticated user to query a list of security groups for an invalid project. This issue creates resources that are unconstrained by the user's quota. If a malicious user were to submit a significant number of requests, this could lead to a denial of service.	6.5	More Details
CVE-2023-26486	Vega is a visualization grammar, a declarative format for creating, saving, and sharing interactive visualization designs. The Vega `scale` expression function has the ability to call arbitrary functions with a single controlled argument. The scale expression function passes a user supplied argument group to getScale, which is then used as if it were an internal context. The context.scales[name].value is accessed from group and called as a function back in scale. This can be exploited to escape the Vega expression sandbox in order to execute arbitrary JavaScript. This issue has been fixed in version 5.13.1.	6.5	More Details
CVE-2023-26047	teler-waf is a Go HTTP middleware that provides teler IDS functionality to protect against web-based attacks. In teler-waf prior to version v0.2.0 is vulnerable to a bypass attack when a specific case-sensitive hex entities payload with special characters such as CR/LF and horizontal tab is used. This vulnerability allows an attacker to execute arbitrary JavaScript code on the victim's browser and compromise the security of the web application. An attacker can exploit this vulnerability to bypass common web attack threat rules in teler-waf and launch cross-site scripting (XSS) attacks. The attacker can execute arbitrary JavaScript code on the victim's browser and steal sensitive information, such as login credentials and session tokens, or take control of the victim's browser and perform malicious actions. This issue has been patched in version 0.2.0.	6.5	More Details
CVE-2023-24130	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey parameter at /goform/WifiBasicSet.	6.5	More Details
CVE-2023-24128	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey2 parameter at /goform/WifiBasicSet.	6.5	More Details
CVE-2021-45478	Improper Handling of Parameters vulnerability in Bordam Information Technologies Library Automation System allows Collect Data as Provided by Users.This issue affects Library Automation System: before 19.2.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45477	Improper Handling of Parameters vulnerability in Bordam Information Technologies Library Automation System allows Collect Data as Provided by Users.This issue affects Library Automation System: before 19.2.	6.5	More Details
CVE-2023-24129	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey4 parameter at /goform/WifiBasicSet.	6.5	More Details
CVE-2023-0952	Improper access controls on entries in Devolutions Server 2022.3.12 and earlier could allow an authenticated user to access sensitive data without proper authorization.	6.5	More Details
CVE-2023-20623	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778.	6.4	More Details
CVE-2023-20625	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532.	6.4	More Details
CVE-2023-22462	Grafana is an open-source platform for monitoring and observability. On 2023-01-01 during an internal audit of Grafana, a member of the security team found a stored XSS vulnerability affecting the core plugin "Text". The stored XSS vulnerability requires several user interactions in order to be fully exploited. The vulnerability was possible due to React's render cycle that will pass though the unsanitized HTML code, but in the next cycle the HTML is cleaned up and saved in Grafana's database. An attacker needs to have the Editor role in order to change a Text panel to include JavaScript. Another user needs to edit the same Text panel, and click on "Markdown" or "HTML" for the code to be executed. This means that vertical privilege escalation is possible, where a user with Editor role can change to a known password for a user having Admin role if the user with Admin role executes malicious JavaScript viewing a dashboard. This issue has been patched in versions 9.2.10 and 9.3.4.	6.4	More Details
CVE-2022-35645	IBM Maximo Asset Management 7.6.1.1, 7.6.1.2, 7.6.1.3 and IBM Maximo Application Suite 8.8 and 8.9 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 230958.	6.4	More Details
CVE-2023-25931	Medtronic identified that the Pelvic Health clinician apps, which are installed on the Smart Programmer mobile device, have a password vulnerability that requires a security update to fix. Not updating could potentially result in unauthorized control of the clinician therapy application, which has greater control over therapy parameters than the patient app. Changes still cannot be made outside of the established therapy parameters of the programmer. For unauthorized access to occur, an individual would need physical access to the Smart Programmer.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1155	The Cost Calculator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the nd_cc_meta_box_cc_price_icon parameter in versions up to, and including, 1.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2008-10003	A vulnerability was found in iGamingModules flashgames 1.1.0. It has been classified as critical. Affected is an unknown function of the file game.php. The manipulation of the argument lid leads to sql injection. It is possible to launch the attack remotely. The name of the patch is 6e57683704885be32eea2ea614f80c9bb8f012c5. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-222288.	6.3	More Details
CVE-2023-22738	vantage6 is a privacy preserving federated learning infrastructure for secure insight exchange. Assigning existing users to a different organizations is currently possible. It may lead to unintended access: if a user from organization A is accidentally assigned to organization B, they will retain their permissions and therefore might be able to access stuff they should not be allowed to access. This issue is patched in version 3.8.0.	6.3	More Details
CVE-2023-1235	Type confusion in DevTools in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted UI interaction. (Chromium security severity: Low)	6.3	More Details
CVE-2015-10087	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in UpThemes Theme DesignFolio Plus 1.2 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of the patch is 53f6ae62878076f99718e5feb589928e83c879a9. It is recommended to apply a patch to fix this issue. The identifier VDB-221809 was assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2021-4328	A vulnerability has been found in 狮子鱼CMS and classified as critical. Affected by this vulnerability is the function goods_detail of the file ApiController.class.php. The manipulation of the argument goods_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The associated identifier of this vulnerability is VDB-222223.	6.3	More Details
CVE-2023-1130	A vulnerability, which was classified as critical, was found in SourceCodester Computer Parts Sales and Inventory System 1.0. This affects an unknown part of the file processlogin. The manipulation of the argument user 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-222105 was assigned to this vulnerability.	6.3	More Details
CVE-2008-10004	A vulnerability was found in Email Registration 5.x-2.1 on Drupal. It has been declared as critical. This vulnerability affects the function email_registration_user of the file email_registration.module. The manipulation of the argument namenew leads to sql injection. The attack can be initiated remotely. Upgrading to version 6.x-1.0 is able to address this issue. The patch is identified as 126c141b7db038c778a2dc931d38766aad8d1112. It is recommended to upgrade the affected component. VDB-222334 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36670	The NEX-Forms. plugin for WordPress is vulnerable to unauthorized disclosure and modification of data in versions up to, and including 7.7.1 due to missing capability checks on several AJAX actions. This makes it possible for authenticated attackers with subscriber level permissions and above to invoke these functions which can be used to perform actions like modify form submission records, deleting files, sending test emails, modifying plugin settings, and more.	6.3	More Details
CVE-2023-1151	A vulnerability was found in SourceCodester Electronic Medical Records System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file administrator.php of the component Cookie Handler. The manipulation of the argument userid 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-222163.	6.3	More Details
CVE-2023-1161	ISO 15765 and ISO 10681 dissector crash in Wireshark 4.0.0 to 4.0.3 and 3.6.0 to 3.6.11 allows denial of service via packet injection or crafted capture file	6.3	More Details
CVE-2023-24733	PMB v7.4.6 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the query parameter at /admin/convert/export_z3950_new.php.	6.1	More Details
CVE-2023-0968	The Watu Quiz plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘dn’, 'email', 'points', and 'date' parameters in versions up to, and including, 3.3.9 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-2023-23313	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2.	6.1	More Details
CVE-2023-23927	Craft is a platform for creating digital experiences. When you insert a payload inside a label name or instruction of an entry type, an cross-site scripting (XSS) happens in the quick post widget on the admin dashboard. This issue has been fixed in version 4.3.7.	6.1	More Details
CVE-2023-24737	PMB v7.4.6 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the query parameter at /admin/convert/export_z3950.php.	6.1	More Details
CVE-2023-24735	PMB v7.4.6 was discovered to contain an open redirect vulnerability via the component /opac_css/pmb.php. This vulnerability allows attackers to redirect victim users to an external domain via a crafted URL.	6.1	More Details
CVE-2023-22432	Open redirect vulnerability exists in web2py versions prior to 2.23.1. When using the tool, a web2py user may be redirected to an arbitrary website by accessing a specially crafted URL. As a result, the user may become a victim of a phishing attack.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35377	Cross Site Scripting vulnerability found in VICIdial v2.14-610c and v.2.10-415c allows attackers execute arbitrary code via the /agc/vicidial.php, agc/vicidial-greay.php, and /vicidial/KHOMP_admin.php parameters.	6.1	More Details
CVE-2021-44196	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in UBIT Information Technologies Student Information Management System.This issue affects Student Information Management System: before 20211126.	6.1	More Details
CVE-2021-44197	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in UBIT Information Technologies Student Information Management System.This issue affects Student Information Management System: before 20211126.	6.1	More Details
CVE-2022-2178	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Saysis Computer Starcities allows Cross-Site Scripting (XSS).This issue affects Starcities: before 1.1.	6.1	More Details
CVE-2023-27641	The REPORT (after z but before a) parameter in wa.exe in L-Soft LISTSERV 16.5 before 17 allows an attacker to conduct XSS attacks via a crafted URL.	6.1	More Details
CVE-2021-36713	Cross Site Scripting (XSS) vulnerability in the DataTables plug-in 1.9.2 for jQuery allows attackers to run arbitrary code via the sBaseName parameter to function _fnCreateCookie. NOTE: 1.9.2 is a version from 2012.	6.1	More Details
CVE-2022-38220	An XSS vulnerability exists within Quest KACE Systems Management Appliance (SMA) through 12.1 that may allow remote injection of arbitrary web script or HTML.	6.1	More Details
CVE-2023-0577	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ASOS Information Technologies SOBIAD allows Cross-Site Scripting (XSS).This issue affects SOBIAD: before 23.02.01.	6.1	More Details
CVE-2023-20104	A vulnerability in the file upload functionality of Cisco Webex App for Web could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending an arbitrary file to a user and persuading that user to browse to a specific URL. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	6.1	More Details
CVE-2022-2837	A flaw was found in coreDNS. This flaw allows a malicious user to redirect traffic intended for external top-level domains (TLD) to a pod they control by creating projects and namespaces that match the TLD.	6.1	More Details
CVE-2023-1106	Cross-site Scripting (XSS) - Reflected in GitHub repository flatpressblog/flatpress prior to 1.3.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20053	A vulnerability in the web-based management interface of Cisco Nexus Dashboard could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. This vulnerability is due to insufficient user input validation. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	6.1	More Details
CVE-2023-20085	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script in the context of the affected interface or access sensitive, browser-based information.	6.1	More Details
CVE-2023-0578	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ASOS Information Technologies Book Cites allows Cross-Site Scripting (XSS).This issue affects Book Cites: before 23.01.05.	6.1	More Details
CVE-2023-20075	Vulnerability in the CLI of Cisco Secure Email Gateway could allow an authenticated, remote attacker to execute arbitrary commands. These vulnerability is due to improper input validation in the CLI. An attacker could exploit this vulnerability by injecting operating system commands into a legitimate command. A successful exploit could allow the attacker to escape the restricted command prompt and execute arbitrary commands on the underlying operating system. To successfully exploit this vulnerability, an attacker would need valid Administrator credentials.	6.0	More Details
CVE-2023-26281	IBM HTTP Server 8.5 used by IBM WebSphere Application Server could allow a remote user to cause a denial of service using a specially crafted URL. IBM X-Force ID: 248296.	5.9	More Details
CVE-2021-20251	A flaw was found in samba. A race condition in the password lockout code may lead to the risk of brute force attacks being successful if special conditions are met.	5.9	More Details
CVE-2023-26470	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. It's possible to make the farm unusable by adding an object to a page with a huge number (e.g. 67108863). Most of the time this will fill the memory allocated to XWiki and make it unusable every time this document is manipulated. This issue has been patched in XWiki 14.0-rc-1.	5.7	More Details
CVE-2023-26510	Ghost 5.35.0 allows authorization bypass: contributors can view draft posts of other users, which is arguably inconsistent with a security policy in which a contributor's draft can only be read by editors until published by an editor. NOTE: the vendor's position is that this behavior has no security impact.	5.7	More Details
CVE-2023-24754	libde265 v1.0.10 was discovered to contain a NULL pointer dereference in the ff_hevc_put_weighted_pred_avg_8_sse function at sse-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23001	In the Linux kernel before 5.16.3, drivers/scsi/ufs/ufs-mediatek.c misinterprets the regulator_get return value (expects it to be NULL in the error case, whereas it is actually an error pointer).	5.5	More Details
CVE-2020-36663	A vulnerability, which was classified as problematic, was found in Artesãos SEOTools up to 0.17.1. This affects the function makeTag of the file OpenGraph.php. The manipulation of the argument value leads to open redirect. Upgrading to version 0.17.2 is able to address this issue. The patch is named ca27cd0edf917e0bc805227013859b8b5a1f01fb. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-222231.	5.5	More Details
CVE-2023-23000	In the Linux kernel before 5.17, drivers/phy/tegra/xusb.c mishandles the tegra_xusb_find_port_node return value. Callers expect NULL in the error case, but an error pointer is used.	5.5	More Details
CVE-2020-36664	A vulnerability has been found in Artesãos SEOTools up to 0.17.1 and classified as problematic. This vulnerability affects the function setTitle of the file SEOMeta.php. The manipulation of the argument title leads to open redirect. Upgrading to version 0.17.2 is able to address this issue. The name of the patch is ca27cd0edf917e0bc805227013859b8b5a1f01fb. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-222232.	5.5	More Details
CVE-2020-36665	A vulnerability was found in Artesãos SEOTools up to 0.17.1 and classified as critical. This issue affects the function eachValue of the file TwitterCards.php. The manipulation of the argument value leads to open redirect. Upgrading to version 0.17.2 is able to address this issue. The identifier of the patch is ca27cd0edf917e0bc805227013859b8b5a1f01fb. It is recommended to upgrade the affected component. The identifier VDB-222233 was assigned to this vulnerability.	5.5	More Details
CVE-2022-48310	An information disclosure vulnerability allows sensitive key material to be included in technical support archives in Sophos Connect versions older than 2.2.90.	5.5	More Details
CVE-2023-24752	libde265 v1.0.10 was discovered to contain a NULL pointer dereference in the ff_hevc_put_hevc_epel_pixels_8_sse function at sse-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input file.	5.5	More Details
CVE-2022-4927	A vulnerability was found in ualbertalib NEOSDiscovery 1.0.70 and classified as problematic. This issue affects some unknown processing of the file app/views/bookmarks/_refworks.html.erb. The manipulation leads to use of web link to untrusted target with window.opener access. The attack may be initiated remotely. Upgrading to version 1.0.71 is able to address this issue. The patch is named abe9f57123e0c278ae190cd7402a623d66c51375. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-222287.	5.5	More Details
CVE-2023-24755	libde265 v1.0.10 was discovered to contain a NULL pointer dereference in the put_weighted_pred_8_fallback function at fallback-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input file.	5.5	More Details
CVE-2023-24756	libde265 v1.0.10 was discovered to contain a NULL pointer dereference in the ff_hevc_put_unweighted_pred_8_sse function at sse-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24757	libde265 v1.0.10 was discovered to contain a NULL pointer dereference in the put_unweighted_pred_16_fallback function at fallback-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input file.	5.5	More Details
CVE-2023-24758	libde265 v1.0.10 was discovered to contain a NULL pointer dereference in the ff_hevc_put_weighted_pred_avg_8_sse function at sse-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input file.	5.5	More Details
CVE-2021-4329	A vulnerability, which was classified as critical, has been found in json-logic-js 2.0.0. Affected by this issue is some unknown functionality of the file logic.js. The manipulation leads to command injection. Upgrading to version 2.0.1 is able to address this issue. The patch is identified as c1dd82f5b15d8a553bb7a0cfa841ab8a11a9c227. It is recommended to upgrade the affected component. VDB-222266 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2021-36689	An issue discovered in com.samourai.wallet.PinEntryActivity.java in Streetside Samourai Wallet 0.99.96i allows attackers to view sensitive information and decrypt data via a brute force attack that uses a recovered samourai.dat file. The PIN is 5 to 8 digits, which may be insufficient in this situation.	5.5	More Details
CVE-2022-36021	Redis is an in-memory database that persists on disk. Authenticated users can use string matching commands (like `SCAN` or `KEYS`) with a specially crafted pattern to trigger a denial-of-service attack on Redis, causing it to hang and consume 100% CPU time. The problem is fixed in Redis versions 6.0.18, 6.2.11, 7.0.9.	5.5	More Details
CVE-2023-1160	Use of Platform-Dependent Third Party Components in GitHub repository cockpit-hq/cockpit prior to 2.4.0.	5.5	More Details
CVE-2023-1165	A vulnerability was found in Zhong Bang CRMEB Java 1.3.4. It has been classified as critical. This affects an unknown part of the file /api/admin/system/store/order/list. The manipulation of the argument keywords leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-222261 was assigned to this vulnerability.	5.5	More Details
CVE-2022-22297	An incomplete filtering of one or more instances of special elements vulnerability [CWE-792] in the command line interpreter of FortiWeb version 6.4.0 through 6.4.1, FortiWeb version 6.3.0 through 6.3.17, FortiWeb all versions 6.2, FortiWeb all versions 6.1, FortiWeb all versions 6.0, FortiRecorder version 6.4.0 through 6.4.3, FortiRecorder all versions 6.0, FortiRecorder all versions 2.7 may allow an authenticated user to read arbitrary files via specially crafted command arguments.	5.5	More Details
CVE-2022-3707	A double-free memory flaw was found in the Linux kernel. The Intel GVT-g graphics driver triggers VGA card system resource overload, causing a fail in the intel_gvt_dma_map_guest_page function. This issue could allow a local user to crash the system.	5.5	More Details
CVE-2023-23005	In the Linux kernel before 6.2, mm/memory-tiers.c misinterprets the alloc_memory_type return value (expects it to be NULL in the error case, whereas it is actually an error pointer). NOTE: this is disputed by third parties because there are no realistic cases in which a user can cause the alloc_memory_type error case to be reached.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25155	Redis is an in-memory database that persists on disk. Authenticated users issuing specially crafted `SRANDMEMBER`, `ZRANDMEMBER`, and `HRANDFIELD` commands can trigger an integer overflow, resulting in a runtime assertion and termination of the Redis server process. This problem affects all Redis versions. Patches were released in Redis version(s) 6.0.18, 6.2.11 and 7.0.9.	5.5	More Details
CVE-2023-23004	In the Linux kernel before 5.19, drivers/gpu/drm/arm/malidp_planes.c misinterprets the get_sg_table return value (expects it to be NULL in the error case, whereas it is actually an error pointer).	5.5	More Details
CVE-2021-4327	A vulnerability was found in SerenityOS. It has been rated as critical. Affected by this issue is the function initialize_typed_array_from_array_buffer in the library Userland/Libraries/LibJS/Runtime/TypedArray.cpp. The manipulation leads to integer overflow. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The patch is identified as f6c6047e49f1517778f5565681fb64750b14bf60. It is recommended to apply a patch to fix this issue. VDB-222074 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2023-23002	In the Linux kernel before 5.16.3, drivers/bluetooth/hci_qca.c misinterprets the devm_gpiod_get_index_optional return value (expects it to be NULL in the error case, whereas it is actually an error pointer).	5.5	More Details
CVE-2023-1264	NULL Pointer Dereference in GitHub repository vim/vim prior to 9.0.1392.	5.5	More Details
CVE-2023-23006	In the Linux kernel before 5.15.13, drivers/net/ethernet/mellanox/mlx5/core/steering/dr_domain.c misinterprets the mlx5_get_uars_page return value (expects it to be NULL in the error case, whereas it is actually an error pointer).	5.5	More Details
CVE-2022-37935	HPE OneView for VMware vCenter, in certain circumstances, may disclose the “HPE OneView” Username and Password.	5.5	More Details
CVE-2023-1107	Cross-site Scripting (XSS) - Stored in GitHub repository flatpressblog/flatpress prior to 1.3.	5.4	More Details
CVE-2023-1241	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.6.	5.4	More Details
CVE-2022-42248	QlikView 12.60.2 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the QvsViewClient functionality.	5.4	More Details
CVE-2021-45479	Improper Neutralization of Input During Web Page Generation vulnerability in Yordam Information Technologies Library Automation System allows Stored XSS.This issue affects Library Automation System: before 19.2.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36398	In moodle, ID numbers displayed in the web service token list required additional sanitizing to prevent a stored XSS risk.	5.4	More Details
CVE-2022-44875	KioWare through 8.33 on Windows sets KioScriptingUrlACL.AclActions.AllowHigh for the about:blank origin, which allows attackers to obtain SYSTEM access via KioUtils.Execute in JavaScript code.	5.4	More Details
CVE-2023-1240	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.6.	5.4	More Details
CVE-2023-1242	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.6.	5.4	More Details
CVE-2021-36399	In Moodle, ID numbers displayed in the quiz override screens required additional sanitizing to prevent a stored XSS risk.	5.4	More Details
CVE-2023-1149	Improper Neutralization of Equivalent Special Elements in GitHub repository btcpayserver/btcpayserver prior to 1.8.0.	5.4	More Details
CVE-2023-25077	Cross-site scripting vulnerability in Authentication Key Settings of EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to 4.1.2-p1, and EC-CUBE 4.2.0 allows a remote authenticated attacker to inject an arbitrary script.	5.4	More Details
CVE-2023-1238	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.6.	5.4	More Details
CVE-2023-0063	The WordPress Shortcodes WordPress plugin through 1.6.36 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-2023-0377	The Scriptless Social Sharing WordPress plugin before 3.2.2 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-2023-1237	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.6.	5.4	More Details
CVE-2023-0212	The Advanced Recent Posts WordPress plugin through 0.6.14 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 Number	Description	Base Score	Reference
CVE-2023-0165	The Cost Calculator WordPress plugin through 1.8 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-2023-0078	The Resume Builder WordPress plugin through 3.1.1 does not sanitize and escape some parameters related to Resume, which could allow users with a role as low as subscriber to perform Stored XSS attacks against higher privilege users	5.4	More Details
CVE-2023-0076	The Download Attachments WordPress plugin before 1.3 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-2023-0069	The WPaudio MP3 Player WordPress plugin through 4.0.2 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-2023-0068	The Product GTIN (EAN, UPC, ISBN) for WooCommerce WordPress plugin through 1.1.1 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-2023-0065	The i2 Pros & Cons WordPress plugin through 1.3.1 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-2023-0064	The eVision Responsive Column Layout Shortcodes WordPress plugin through 2.3 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-2023-26056	XWiki Platform is a generic wiki platform. Starting in version 3.0-milestone-1, it's possible to execute a script with the right of another user, provided the target user does not have programming right. The problem has been patched in XWiki 14.8-rc-1, 14.4.5, and 13.10.10. There are no known workarounds for this issue.	5.4	More Details
CVE-2023-1244	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.6.	5.4	More Details
CVE-2023-1104	Cross-site Scripting (XSS) - Stored in GitHub repository flatpressblog/flatpress prior to 1.3.	5.4	More Details
CVE-2023-22838	Cross-site scripting vulnerability in Product List Screen and Product Detail Screen of EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to 4.1.2-p1, and EC-CUBE 4.2.0 allows a remote authenticated attacker to inject an arbitrary script.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46806	Cross-Site Request Forgery (CSRF) vulnerability in VillaTheme Cart All In One For WooCommerce plugin <= 1.1.10 leading to cart modification.	5.4	More Details
CVE-2023-23974	Cross-Site Request Forgery (CSRF) vulnerability in Fullworks Quick Event Manager plugin <= 9.7.4 affecting all registration actions (delete, delete all, edit, update).	5.4	More Details
CVE-2023-23984	Cross-Site Request Forgery (CSRF) vulnerability in Wow-Company Bubble Menu – circle floating menu plugin <= 3.0.1 leading to form deletion.	5.4	More Details
CVE-2022-45068	Cross-Site Request Forgery (CSRF) vulnerability in Mercado Pago Mercado Pago payments for WooCommerce plugin <= 6.3.1.	5.4	More Details
CVE-2022-45804	Cross-Site Request Forgery (CSRF) vulnerability in RoboSoft Photo Gallery, Images, Slider in Rbs Image Gallery plugin <= 3.2.9 leading to galleries hierarchy change, included plugin deactivate & activate.	5.4	More Details
CVE-2022-46797	Cross-Site Request Forgery (CSRF) vulnerability in Conversios All-in-one Google Analytics, Pixels and Product Feed Manager for WooCommerce plugin <= 5.2.3 leads to plugin settings change.	5.4	More Details
CVE-2023-1115	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.18.	5.4	More Details
CVE-2023-1116	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.18.	5.4	More Details
CVE-2023-1117	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.18.	5.4	More Details
CVE-2022-27490	A exposure of sensitive information to an unauthorized actor in Fortinet FortiManager version 6.0.0 through 6.0.4, FortiAnalyzer version 6.0.0 through 6.0.4, FortiPortal version 6.0.0 through 6.0.9, 5.3.0 through 5.3.8, 5.2.x, 5.1.0, 5.0.x, 4.2.x, 4.1.x, FortiSwitch version 7.0.0 through 7.0.4, 6.4.0 through 6.4.10, 6.2.x, 6.0.x allows an attacker which has obtained access to a restricted administrative account to obtain sensitive information via `diagnose debug` commands.	5.4	More Details
CVE-2023-26608	SOLDR (System of Orchestration, Lifecycle control, Detection and Response) 1.1.0 allows stored XSS via the module editor.	5.4	More Details
CVE-2023-26491	RSSHub is an open source and extensible RSS feed generator. When the URL parameters contain certain special characters, it returns an error page that does not properly handle XSS vulnerabilities, allowing for the execution of arbitrary JavaScript code. Users who access the deliberately constructed URL are affected. This vulnerability was fixed in version c910c4d28717fb860fbe064736641f379fab2c91. Please upgrade to this or a later version, there are no known workarounds.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22438	Cross-site scripting vulnerability in Contents Management of EC-CUBE 4 series (EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to 4.1.2-p1, and EC-CUBE 4.2.0), EC-CUBE 3 series (EC-CUBE 3.0.0 to 3.0.18-p5), and EC-CUBE 2 series (EC-CUBE 2.11.0 to 2.11.5, EC-CUBE 2.12.0 to 2.12.6, EC-CUBE 2.13.0 to 2.13.5, and EC-CUBE 2.17.0 to 2.17.2) allows a remote authenticated attacker to inject an arbitrary script.	5.4	More Details
CVE-2022-46798	Cross-Site Request Forgery (CSRF) vulnerability in HasThemes ShopLentor plugin <= 2.5.1 leading to plugin settings change.	5.4	More Details
CVE-2022-46805	Cross-Site Request Forgery (CSRF) vulnerability in Lauri Karisola / WP Trio Conditional Shipping for WooCommerce plugin <= 2.3.1 leading to activation/deactivation of plugin rulesets.	5.4	More Details
CVE-2023-1147	Cross-site Scripting (XSS) - Stored in GitHub repository flatpressblog/flatpress prior to 1.3.	5.4	More Details
CVE-2023-26954	onekeyadmin v1.3.9 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the User Group module.	5.4	More Details
CVE-2023-1245	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.6.	5.4	More Details
CVE-2020-36667	The JetBackup – WP Backup, Migrate & Restore plugin for WordPress is vulnerable to unauthorized back-up location changes in versions up to, and including 1.4.1 due to a lack of proper capability checking on the backup_guard_cloud_dropbox, backup_guard_cloud_gdrive, and backup_guard_cloud_oneDrive functions. This makes it possible for authenticated attackers, with minimal permissions, such as a subscriber to change to location of back-ups and potentially steal sensitive information from them.	5.4	More Details
CVE-2023-1181	Cross-site Scripting (XSS) - Stored in GitHub repository icret/easyimages2.0 prior to 2.6.7.	5.4	More Details
CVE-2023-20069	A vulnerability in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network (EPN) Manager could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker would need to have valid credentials to access the web-based management interface of the affected device.	5.4	More Details
CVE-2023-1146	Cross-site Scripting (XSS) - Generic in GitHub repository flatpressblog/flatpress prior to 1.3.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26955	onekeyadmin v1.3.9 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Admin Group module.	5.4	More Details
CVE-2023-20088	A vulnerability in the nginx configurations that are provided as part of the VPN-less reverse proxy for Cisco Finesse could allow an unauthenticated, remote attacker to create a denial of service (DoS) condition for new and existing users who are connected through a load balancer. This vulnerability is due to improper IP address filtering by the reverse proxy. An attacker could exploit this vulnerability by sending a series of unauthenticated requests to the reverse proxy. A successful exploit could allow the attacker to cause all current traffic and subsequent requests to the reverse proxy through a load balancer to be dropped, resulting in a DoS condition.	5.3	More Details
CVE-2022-41329	An exposure of sensitive information to an unauthorized actor vulnerability [CWE-200] in Fortinet FortiProxy version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.7, FortiOS version 7.2.0 through 7.2.3 and 7.0.0 through 7.0.9 allows an unauthenticated attackers to obtain sensitive logging informations on the device via crafted HTTP GET requests.	5.3	More Details
CVE-2021-36400	In Moodle, insufficient capability checks made it possible to remove other users' calendar URL subscriptions.	5.3	More Details
CVE-2023-0085	The Metform Elementor Contact Form Builder plugin for WordPress is vulnerable to reCaptcha Bypass in versions up to, and including, 3.2.1. This is due to insufficient server side checking on the captcha value submitted during a form submission. This makes it possible for unauthenticated attackers to bypass Captcha restrictions and for attackers to utilize bots to submit forms.	5.3	More Details
CVE-2023-1003	A vulnerability, which was classified as critical, was found in Typora up to 1.5.5 on Windows. Affected is an unknown function of the component WSH JScript Handler. The manipulation leads to code injection. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. Upgrading to version 1.5.8 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-221736.	5.3	More Details
CVE-2021-36397	In Moodle, insufficient capability checks meant message deletions were not limited to the current user.	5.3	More Details
CVE-2023-25806	OpenSearch Security is a plugin for OpenSearch that offers encryption, authentication and authorization. There is an observable discrepancy in the authentication response time between calls where the user provided exists and calls where it does not. This issue only affects calls using the internal basic identity provider (IdP), and not other externally configured IdPs. Patches were released in versions 1.3.9 and 2.6.0, there are no workarounds.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20052	On Feb 15, 2023, the following vulnerability in the ClamAV scanning library was disclosed: A vulnerability in the DMG file parser of ClamAV versions 1.0.0 and earlier, 0.105.1 and earlier, and 0.103.7 and earlier could allow an unauthenticated, remote attacker to access sensitive information on an affected device. This vulnerability is due to enabling XML entity substitution that may result in XML external entity injection. An attacker could exploit this vulnerability by submitting a crafted DMG file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to leak bytes from any file that may be read by the ClamAV scanning process.	5.3	More Details
CVE-2022-20952	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance, formerly known as Cisco Web Security Appliance (WSA), could allow an unauthenticated, remote attacker to bypass a configured rule, thereby allowing traffic onto a network that should have been blocked. This vulnerability exists because malformed, encoded traffic is not properly detected. An attacker could exploit this vulnerability by connecting through an affected device to a malicious server and receiving malformed HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device.	5.3	More Details
CVE-2017-20181	A vulnerability classified as critical was found in hgzojer Vocable Trainer up to 1.3.0 on Android. This vulnerability affects unknown code of the file src/at/hgz/vocabletrainer/VocableTrainerProvider.java. The manipulation leads to path traversal. Attacking locally is a requirement. Upgrading to version 1.3.1 is able to address this issue. The name of the patch is accf6838078f8eb105cfc7865aba5c705fb68426. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-222328.	5.3	More Details
CVE-2023-0847	The Sub-IoT implementation of the DASH 7 Alliance protocol has a vulnerability that can lead to an out-of-bounds write prior to implementation version 0.5.0. If the protocol has been compiled using default settings, this will only grant the attacker access to allocated but unused memory. However, if it was configured using non-default settings, there is the possibility that exploiting this vulnerability could lead to system crashes and remote code execution.	5.3	More Details
CVE-2022-39228	vantage6 is a privacy preserving federated learning infrastructure for secure insight exchange. vantage6 does not inform the user of wrong username/password combination if the username actually exists. This is an attempt to prevent bots from obtaining usernames. However, if a wrong password is entered a number of times, the user account is blocked temporarily. This issue has been fixed in version 3.8.0.	5.3	More Details
CVE-2023-1263	The CMP – Coming Soon & Maintenance plugin for WordPress is vulnerable to Information Exposure in versions up to, and including, 4.1.6 via the cmp_get_post_detail function. This can allow unauthenticated individuals to obtain the contents of any non-password-protected, published post or page even when maintenance mode is enabled.	5.3	More Details
CVE-2023-0330	A vulnerability in the lsi53c895a device affects the latest version of qemu. A DMA-MMIO reentrancy problem may lead to memory corruption bugs like stack overflow or use-after-free.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26483	gosaml2 is a Pure Go implementation of SAML 2.0. SAML Service Providers using this library for SAML authentication support are likely susceptible to Denial of Service attacks. A bug in this library enables attackers to craft a `deflate`-compressed request which will consume significantly more memory during processing than the size of the original request. This may eventually lead to memory exhaustion and the process being killed. The maximum compression ratio achievable with `deflate` is 1032:1, so by limiting the size of bodies passed to gosaml2, limiting the rate and concurrency of calls, and ensuring that lots of memory is available to the process it _may_ be possible to help Go's garbage collector "keep up". Implementors are encouraged not to rely on this. This issue is fixed in version 0.9.0.	5.3	More Details
CVE-2023-22858	An Improper Access Control vulnerability in BlogEngine.NET 3.3.8.0, allows unauthenticated visitors to access the files of unpublished blogs.	5.3	More Details
CVE-2021-36402	In Moodle, Users' names required additional sanitizing in the account confirmation email, to prevent a self-registration phishing risk.	5.3	More Details
CVE-2023-25819	Discourse is an open source platform for community discussion. Tags that are normally private are showing in metadata. This affects any site running the `tests-passed` or `beta` branches >= 3.1.0.beta2. The issue is patched in the latest `beta` and `tests-passed` version of Discourse.	5.3	More Details
CVE-2021-36403	In Moodle, in some circumstances, email notifications of messages could have the link back to the original message hidden by HTML, which may pose a phishing risk.	5.3	More Details
CVE-2023-0734	Improper Authorization in GitHub repository wallabag/wallabag prior to 2.5.4.	5.3	More Details
CVE-2023-0460	The YouTube Embedded 1.2 SDK binds to a service within the YouTube Main App. After binding, a remote context is created with the flags Context.CONTEXT_INCLUDE_CODE | Context.CONTEXT_IGNORE_SECURITY. This allows the client app to remotely load code from YouTube Main App by retrieving the Main App's ClassLoader. A potential vulnerability in the binding logic used by the client SDK where the SDK ends up calling bindService() on a malicious app rather than YT Main App. This creates a vulnerability where the SDK can load the malicious app's ClassLoader instead, allowing the malicious app to load arbitrary code into the calling app whenever the embedded SDK is invoked. In order to trigger this vulnerability, an attacker must masquerade the Youtube app and install it on a device, have a second app that uses the Embedded player and typically distribute both to the victim outside of the Play Store.	5.1	More Details
CVE-2023-26492	Directus is a real-time API and App dashboard for managing SQL database content. Directus is vulnerable to Server-Side Request Forgery (SSRF) when importing a file from a remote web server (POST to `/files/import`). An attacker can bypass the security controls by performing a DNS rebinding attack and view sensitive data from internal servers or perform a local port scan. An attacker can exploit this vulnerability to access highly sensitive internal server(s) and steal sensitive information. This issue was fixed in version 9.23.0.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2015-10088	A vulnerability, which was classified as critical, was found in ayttm up to 0.5.0.89. This affects the function http_connect in the library libproxy/proxy.c. The manipulation leads to format string. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The patch is named 40e04680018614a7d2b68566b261b061a0597046. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-222267.	5.0	More Details
CVE-2022-4862	Rendering of HTML provided by another authenticated user is possible in browser on M-Files Web before 22.12.12140.3. This allows the content to steal user sensitive information. This issue affects M-Files New Web: before 22.12.12140.3.	5.0	More Details
CVE-2023-25230	A Server-Side Request Forgery (SSRF) in loonflow r2.0.14 allows attackers to force the application to make arbitrary requests via manipulation of the hook_url parameter.	4.9	More Details
CVE-2023-22777	An authenticated information disclosure vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files in the underlying operating system.	4.9	More Details
CVE-2023-22776	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files.	4.9	More Details
CVE-2021-36401	In Moodle, ID numbers exported in HTML data formats required additional sanitizing to prevent a local stored XSS risk.	4.8	More Details
CVE-2023-1243	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.6.	4.8	More Details
CVE-2023-22778	A vulnerability in the ArubaOS web management interface could allow an authenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface.	4.8	More Details
CVE-2023-26953	onekeyadmin v1.3.9 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Add Administrator module.	4.8	More Details
CVE-2023-1212	Cross-site Scripting (XSS) - Stored in GitHub repository phpipam/phpipam prior to v1.5.2.	4.8	More Details
CVE-2023-1239	Cross-site Scripting (XSS) - Reflected in GitHub repository answerdev/answer prior to 1.0.6.	4.8	More Details
CVE-2023-1148	Cross-site Scripting (XSS) - Stored in GitHub repository flatpressblog/flatpress prior to 1.3.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1190	A vulnerability was found in xiaozhuai imageinfo up to 3.0.3. It has been rated as problematic. Affected by this issue is some unknown functionality of the file imageinfo.hpp. The manipulation leads to buffer overflow. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. VDB-222362 is the identifier assigned to this vulnerability.	4.8	More Details
CVE-2023-1197	Cross-site Scripting (XSS) - Stored in GitHub repository uvdesk/community-skeleton prior to 1.1.0.	4.8	More Details
CVE-2023-1112	A vulnerability was found in Drag and Drop Multiple File Upload Contact Form 7 5.0.6.1 on WordPress. It has been classified as critical. Affected is an unknown function of the file admin-ajax.php. The manipulation of the argument upload_name leads to relative path traversal. 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-222072.	4.7	More Details
CVE-2023-1191	A vulnerability classified as problematic has been found in fastcms. This affects an unknown part of the file admin/TemplateController.java of the component ZIP File Handler. The manipulation leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The associated identifier of this vulnerability is VDB-222363.	4.7	More Details
CVE-2023-1184	A vulnerability, which was classified as problematic, has been found in ECshop up to 4.1.8. Affected by this issue is some unknown functionality of the file admin/database.php of the component Backup Database Handler. The manipulation leads to unrestricted upload. 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-222356.	4.7	More Details
CVE-2023-1185	A vulnerability, which was classified as problematic, was found in ECshop up to 4.1.8. This affects an unknown part of the component New Product Handler. The manipulation leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-222357 was assigned to this vulnerability.	4.7	More Details
CVE-2015-10091	A vulnerability has been found in ByWater Solutions bywater-koha-xslt and classified as critical. This vulnerability affects the function StringSearch of the file admin/systempreferences.pl. The manipulation of the argument name leads to sql injection. The attack can be initiated remotely. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The patch is identified as 9513b93c828dfbc4413f9e0df63647401aaf4e58. It is recommended to apply a patch to fix this issue. VDB-222322 is the identifier assigned to this vulnerability.	4.7	More Details
CVE-2014-125091	A vulnerability has been found in codepeople cp-polls Plugin 1.0.1 on WordPress and classified as critical. This vulnerability affects unknown code of the file cp-admin-int-message-list.inc.php. The manipulation of the argument lu leads to sql injection. The attack can be initiated remotely. Upgrading to version 1.0.2 is able to address this issue. The name of the patch is 6d7168cbf12d1c183bacc5cd5678f6f5b0d518d2. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-222268.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27672	When SMT is enabled, certain AMD processors may speculatively execute instructions using a target from the sibling thread after an SMT mode switch potentially resulting in information disclosure.	4.7	More Details
CVE-2022-40633	A malicious actor can clone access cards used to open control cabinets secured with Rittal CMC III locks.	4.6	More Details
CVE-2017-20180	A vulnerability classified as critical has been found in Zerocoin libzerocoin. Affected is the function CoinSpend::CoinSpend of the file CoinSpend.cpp of the component Proof Handler. The manipulation leads to insufficient verification of data authenticity. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The patch is identified as ce103a09ec079d0a0ed95475992348bed6e860de. It is recommended to apply a patch to fix this issue. VDB-222318 is the identifier assigned to this vulnerability.	4.6	More Details
CVE-2023-23776	An exposure of sensitive information to an unauthorized actor [CWE-200] vulnerability in FortiAnalyzer versions 7.2.0 through 7.2.1, 7.0.0 through 7.0.4 and 6.4.0 through 6.4.10 may allow a remote authenticated attacker to read the client machine password in plain text in a heartbeat response when a log-fetch request is made from the FortiAnalyzer	4.6	More Details
CVE-2022-2835	A flaw was found in coreDNS. This flaw allows a malicious user to reroute internal calls to some internal services that were accessed by the FQDN in a format of <service>.<namespace>.svc.	4.4	More Details
CVE-2023-20645	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628609; Issue ID: ALPS07628609.	4.4	More Details
CVE-2023-20644	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603.	4.4	More Details
CVE-2023-20646	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536.	4.4	More Details
CVE-2023-20647	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547.	4.4	More Details
CVE-2023-20648	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20649	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607.	4.4	More Details
CVE-2023-20651	In apu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629576; Issue ID: ALPS07629576.	4.4	More Details
CVE-2023-20635	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028.	4.4	More Details
CVE-2023-23973	Cross-Site Request Forgery (CSRF) vulnerability in a3rev Software Contact Us Page – Contact People plugin <= 3.7.0.	4.3	More Details
CVE-2022-38468	Cross-Site Request Forgery (CSRF) vulnerability in Imagely WordPress Gallery Plugin – NextGEN Gallery plugin <= 3.28 leading to thumbnail alteration.	4.3	More Details
CVE-2023-1229	Inappropriate implementation in Permission prompts in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2023-1225	Insufficient policy enforcement in Navigation in Google Chrome on iOS prior to 111.0.5563.64 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2020-36668	The JetBackup – WP Backup, Migrate & Restore plugin for WordPress is vulnerable to sensitive information disclosure in versions up to, and including, 1.4.0 due to a lack of proper capability checking on the backup_guard_get_manual_modal function called via an AJAX action. This makes it possible for subscriber-level attackers, and above, to invoke the function and obtain database table information.	4.3	More Details
CVE-2022-46257	An information disclosure vulnerability was identified in GitHub Enterprise Server that allowed private repositories to be added to a GitHub Actions runner group via the API by a user who did not have access to those repositories, resulting in the repository names being shown in the UI. To exploit this vulnerability, an attacker would need access to the GHES instance, permissions to modify GitHub Actions runner groups, and successfully guess the obfuscated ID of private repositories. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.7 and was fixed in versions 3.3.17, 3.4.12, 3.5.9, 3.6.5. This vulnerability was reported via the GitHub Bug Bounty program.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27481	Directus is a real-time API and App dashboard for managing SQL database content. In versions prior to 9.16.0 users with read access to the `password` field in `directus_users` can extract the argon2 password hashes by brute forcing the export functionality combined with a `_starts_with` filter. This allows the user to enumerate the password hashes. Accounts cannot be taken over unless the hashes can be reversed which is unlikely with current hardware. This problem has been patched by preventing any hashed/concealed field to be filtered against with the `_starts_with` or other string operator in version 9.16.0. Users are advised to upgrade. Users unable to upgrade may mitigate this issue by ensuring that no user has `read` access to the `password` field in `directus_users`.	4.3	More Details
CVE-2023-1236	Inappropriate implementation in Internals in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to spoof the origin of an iframe via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2023-1234	Inappropriate implementation in Intents in Google Chrome on Android prior to 111.0.5563.64 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2023-1230	Inappropriate implementation in WebApp Installs in Google Chrome on Android prior to 111.0.5563.64 allowed an attacker who convinced a user to install a malicious WebApp to spoof the contents of the PWA installer via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2023-1233	Insufficient policy enforcement in Resource Timing in Google Chrome prior to 111.0.5563.64 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from API via a crafted Chrome Extension. (Chromium security severity: Low)	4.3	More Details
CVE-2022-47148	Cross-Site Request Forgery (CSRF) vulnerability in WP Overnight PDF Invoices & Packing Slips for WooCommerce plugin <= 3.2.5 leading to popup dismiss.	4.3	More Details
CVE-2022-4931	The BackupWordPress plugin for WordPress is vulnerable to information disclosure in versions up to, and including 3.12. This is due to missing authorization on the heartbeat_received() function that triggers on WordPress heartbeat. This makes it possible for authenticated attackers, with subscriber-level permissions and above to retrieve back-up paths that can subsequently be used to download the back-up.	4.3	More Details
CVE-2022-4932	The Total Upkeep plugin for WordPress is vulnerable to information disclosure in versions up to, and including 1.14.13. This is due to missing authorization on the heartbeat_received() function that triggers on WordPress heartbeat. This makes it possible for authenticated attackers, with subscriber-level permissions and above to retrieve back-up paths that can subsequently be used to download the back-up.	4.3	More Details
CVE-2022-40198	Cross-Site Request Forgery (CSRF) vulnerability in StandaloneTech TeraWallet – For WooCommerce plugin <= 1.3.24 leading to plugin settings change.	4.3	More Details
CVE-2023-1232	Insufficient policy enforcement in Resource Timing in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to obtain potentially sensitive information from API via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27485	thmmniii/fbs-core is an open source feedback system for students. In versions prior to 1.5.3 when querying `subresults`, it is possible to query `subresults` from other users due to insufficient authorisation. This is only possible for logged-in users and it is not possible to associate the subresults with a specific user. This bug was fixed in commit `f1ae67d8bb2`and released with version 1.5.3. Users are advised to upgrade. There are no known workarounds for this issue.	4.3	More Details
CVE-2023-1224	Insufficient policy enforcement in Web Payments API in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2020-5026	IBM Financial Transaction Manager for Digital Payments for Multi-Platform 3.2.0 through 3.2.7 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 193662.	4.3	More Details
CVE-2020-5001	IBM Financial Transaction Manager 3.2.0 through 3.2.7 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 192953.	4.3	More Details
CVE-2023-0328	The WPCode WordPress plugin before 2.0.7 does not have adequate privilege checks in place for several AJAX actions, only checking the nonce. This may lead to allowing any authenticated user who can edit posts to call the endpoints related to WPCode Library authentication (such as update and delete the auth key).	4.3	More Details
CVE-2022-48364	The undo_mark_statuses_as_sensitive method in app/services/approve_appeal_service.rb in Mastodon 3.5.x before 3.5.3 does not use the server's representative account, resulting in moderator identity disclosure when a moderator approves the appeal of a user whose status update was marked as sensitive.	4.3	More Details
CVE-2023-1221	Insufficient policy enforcement in Extensions API in Google Chrome prior to 111.0.5563.64 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension. (Chromium security severity: Medium)	4.3	More Details
CVE-2023-1223	Insufficient policy enforcement in Autofill in Google Chrome on Android prior to 111.0.5563.64 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2023-1228	Insufficient policy enforcement in Intents in Google Chrome on Android prior to 111.0.5563.64 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2022-48309	A CSRF vulnerability allows malicious websites to retrieve logs and technical support archives in Sophos Connect versions older than 2.2.90.	4.3	More Details
CVE-2023-1231	Inappropriate implementation in Autofill in Google Chrome on Android prior to 111.0.5563.64 allowed a remote attacker to potentially spoof the contents of the omnibox via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22847	Information disclosure vulnerability exists in pg_ivm versions prior to 1.5.1. An Incrementally Maintainable Materialized View (IMMV) created by pg_ivm may reflect rows with Row-Level Security that the owner of the IMMV should not have access to. As a result, information in tables protected by Row-Level Security may be retrieved by a user who is not authorized to access it.	4.3	More Details
CVE-2023-22381	A code injection vulnerability was identified in GitHub Enterprise Server that allowed setting arbitrary environment variables from a single environment variable value in GitHub Actions when using a Windows based runner. To exploit this vulnerability, an attacker would need existing permission to control the value of environment variables for use with GitHub Actions. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.8.0 and was fixed in versions 3.4.15, 3.5.12, 3.6.8, 3.7.5. This vulnerability was reported via the GitHub Bug Bounty program.	4.1	More Details
CVE-2023-20620	In adsp, there is a possible escalation of privilege due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07554558; Issue ID: ALPS07554558.	4.1	More Details
CVE-2023-25611	A improper neutralization of formula elements in a CSV file vulnerability in Fortinet FortiAnalyzer 6.4.0 - 6.4.9, 7.0.0 - 7.0.5, and 7.2.0 - 7.2.1 allows local attacker to execute unauthorized code or commands via inserting spreadsheet formulas in macro names.	4.0	More Details
CVE-2023-23003	In the Linux kernel before 5.16, tools/perf/util/expr.c lacks a check for the hashmap__new return value.	4.0	More Details
CVE-2023-22481	FreshRSS is a self-hosted RSS feed aggregator. When using the greader API, the provided password is logged in clear in `users/_/log_api.txt` in the case where the authentication fails. The issues occurs in `authorizationToUser()` in `greader.php`. If there is an issue with the request or the credentials, `unauthorized()` or `badRequest()` is called. Both these functions are printing the return of `debugInfo()` in the logs. `debugInfo()` will return the content of the request. By default, this will be saved in `users/_/log_api.txt` and if the const `COPY_LOG_TO_SYSLOG` is true, in syslogs as well. Exploiting this issue requires having access to logs produced by FreshRSS. Using the information from the logs, a malicious individual could get users' API keys (would be displayed if the users fills in a bad username) or passwords.	4.0	More Details
CVE-2023-23939	Azure/setup-kubectl is a GitHub Action for installing Kubectl. This vulnerability only impacts versions before version 3. An insecure temporary creation of a file allows other actors on the Actions runner to replace the Kubectl binary created by this action because it is world writable. This Kubectl tool installer runs `fs.chmodSync(kubectlPath, 777)` to set permissions on the Kubectl binary, however, this allows any local user to replace the Kubectl binary. This allows privilege escalation to the user that can also run kubectl, most likely root. This attack is only possible if an attacker somehow breached the GitHub actions runner or if a user is utilizing an Action that maliciously executes this attack. This has been fixed and released in all versions `v3` and later. 775 permissions are used instead. Users are advised to upgrade. There are no known workarounds for this issue.	3.9	More Details
CVE-2022-41862	In PostgreSQL, a modified, unauthenticated server can send an unterminated string during the establishment of Kerberos transport encryption. In certain conditions a server can cause a libpq client to over-read and report an error message containing uninitialized bytes.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26108	Versions of the package @nestjs/core before 9.0.5 are vulnerable to Information Exposure via the StreamableFile pipe. Exploiting this vulnerability is possible when the client cancels a request while it is streaming a StreamableFile, the stream wrapped by the StreamableFile will be kept open.	3.7	More Details
CVE-2023-26052	Saleor is a headless, GraphQL commerce platform delivering personalized shopping experiences. Some internal Python exceptions are not handled properly and thus are returned in API as error messages. Some messages might contain sensitive information like infrastructure details in unauthenticated requests. This issue has been patched in versions 3.1.48, 3.7.59, 3.8.0, 3.9.27, 3.10.14 and 3.11.12.	3.7	More Details
CVE-2015-10095	A vulnerability classified as problematic has been found in woo-popup Plugin up to 1.2.2 on WordPress. This affects an unknown part of the file admin/class-woo-popup-admin.php. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 1.3.0 is able to address this issue. The patch is named 7c76ac78f3e16015991b612ff4fa616af4ce9292. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-222327.	3.5	More Details
CVE-2014-125090	A vulnerability was found in Media Downloader Plugin 0.1.992 on WordPress. It has been declared as problematic. This vulnerability affects the function dl_file_resumable of the file getfile.php. The manipulation of the argument file leads to cross site scripting. The attack can be initiated remotely. Upgrading to version 0.1.993 is able to address this issue. The patch is identified as 77beb720c682b9300035ab5f96eee225181d8a92. It is recommended to upgrade the affected component. VDB-222262 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-1254	A vulnerability has been found in SourceCodester Health Center Patient Record Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file birthing_print.php. The manipulation of the argument birth_id 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-222484.	3.5	More Details
CVE-2022-4929	A vulnerability was found in icplayer up to 0.818. It has been rated as problematic. Affected by this issue is some unknown functionality of the file addons/Commons/src/tts-utils.js. The manipulation leads to cross site scripting. The attack may be launched remotely. Upgrading to version 0.819 is able to address this issue. The patch is identified as fa785969f213c76384f1fe67d47b17d57fcc60c8. It is recommended to upgrade the affected component. VDB-222290 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2015-10092	A vulnerability was found in Qtranslate Slug Plugin up to 1.1.16 on WordPress. It has been classified as problematic. Affected is the function add_slug_meta_box of the file includes/class-qtranslate-slug.php. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 1.1.17 is able to address this issue. The name of the patch is 74b3932696f9868e14563e51b7d0bb68c53bf5e4. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-222324.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4930	A vulnerability classified as problematic was found in nuxsmin sysPass up to 3.2.4. Affected by this vulnerability is an unknown functionality of the component URL Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. Upgrading to version 3.2.5 is able to address this issue. The patch is named 4da4d031732ecca67519851fd0c34597dbb8ee55. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-222319.	3.5	More Details
CVE-2015-10090	A vulnerability, which was classified as problematic, has been found in Landing Pages Plugin up to 1.8.7 on WordPress. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. The attack may be launched remotely. Upgrading to version 1.8.8 is able to address this issue. The name of the patch is c8e22c1340c11fedfb0a0a67ea690421bdb62b94. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-222320.	3.5	More Details
CVE-2014-125092	A vulnerability was found in MaxButtons Plugin up to 1.26.0 on WordPress and classified as problematic. This issue affects the function maxbuttons_strip_px of the file includes/maxbuttons-button.php. The manipulation of the argument button_id leads to cross site scripting. The attack may be initiated remotely. Upgrading to version 1.26.1 is able to address this issue. The patch is named e74564c9e3b7429808e317f4916bd1c26ef0b806. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-222323.	3.5	More Details
CVE-2006-10001	A vulnerability, which was classified as problematic, was found in Subscribe to Comments Plugin up to 2.0.7 on WordPress. This affects an unknown part of the file subscribe-to-comments.php. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 2.0.8 is able to address this issue. The identifier of the patch is 9683bdf462fcac2f32b33be98f0b96497fbd1bb6. It is recommended to upgrade the affected component. The identifier VDB-222321 was assigned to this vulnerability.	3.5	More Details
CVE-2015-10089	A vulnerability classified as problematic has been found in flame.js. This affects an unknown part. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The patch is named e6c49b5f6179e31a534b7c3264e1d36aa99728ac. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-222291.	3.5	More Details
CVE-2023-1200	A vulnerability was found in ehuacui bbs. It has been declared as problematic. This vulnerability affects unknown code. The manipulation of the argument username leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The identifier of this vulnerability is VDB-222388.	3.5	More Details
CVE-2022-4928	A vulnerability was found in icplayer up to 0.819. It has been declared as problematic. Affected by this vulnerability is the function AddonText_Selection_create of the file addons/Text_Selection/src/presenter.js. The manipulation leads to cross site scripting. The attack can be launched remotely. Upgrading to version 0.820 is able to address this issue. The identifier of the patch is 2223628e6db1df73f6d633d2c0422d995990f0a3. It is recommended to upgrade the affected component. The identifier VDB-222289 was assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1156	A vulnerability classified as problematic was found in SourceCodester Health Center Patient Record Management System 1.0. This vulnerability affects unknown code of the file admin/fecalysis_form.php. The manipulation of the argument itr_no 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-222220.	3.5	More Details
CVE-2023-1131	A vulnerability has been found in SourceCodester Computer Parts Sales and Inventory System 1.0 and classified as problematic. This vulnerability affects unknown code of the file customer.php. The manipulation of the argument FIRST_NAME/LAST_NAME/PHONE_NUMBER leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-222106 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-1180	A vulnerability has been found in SourceCodester Health Center Patient Record Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file hematology_print.php. The manipulation of the argument hem_id 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-222331.	3.5	More Details
CVE-2023-1179	A vulnerability, which was classified as problematic, was found in SourceCodester Computer Parts Sales and Inventory System 1.0. Affected is an unknown function of the component Add Supplier Handler. The manipulation of the argument company_name/province/city/phone_number 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-222330 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2008-10002	A vulnerability has been found in cfire24 ajaxlife up to 0.3.2 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting. The attack can be initiated remotely. Upgrading to version 0.3.3 is able to address this issue. The patch is identified as 9fb53b67312fe3f4336e01c1e3e1bedb4be0c1c8. It is recommended to upgrade the affected component. VDB-222286 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-1188	A vulnerability was found in FabulaTech Webcam for Remote Desktop 2.8.42. It has been classified as problematic. Affected is the function 0x222018 in the library ftwebcam.sys of the component IoControlCode Handler. The manipulation leads to denial of service. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-222360.	3.3	More Details
CVE-2021-4326	A vulnerability in Imperative framework which allows already-privileged local actors to execute arbitrary shell commands via plugin install/update commands, or maliciously formed environment variables. Impacts Zowe CLI.	3.3	More Details
CVE-2022-4901	Multiple stored XSS vulnerabilities in Sophos Connect versions older than 2.2.90 allow Javascript code to run in the local UI via a malicious VPN configuration that must be manually loaded by the victim.	3.3	More Details
CVE-2023-1186	A vulnerability has been found in FabulaTech Webcam for Remote Desktop 2.8.42 and classified as problematic. This vulnerability affects the function 0x222010/0x222018 in the library ftwebcam.sys of the component IOCTL Handler. The manipulation leads to null pointer dereference. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. VDB-222358 is the identifier assigned to this vulnerability.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1187	A vulnerability was found in FabulaTech Webcam for Remote Desktop 2.8.42 and classified as problematic. This issue affects some unknown processing in the library ftwebcam.sys of the component Global Variable Handler. The manipulation leads to denial of service. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-222359.	3.3	More Details
CVE-2023-1189	A vulnerability was found in WiseCleaner Wise Folder Hider 4.4.3.202. It has been declared as problematic. Affected by this vulnerability is the function 0x222400/0x222404/0x222410 in the library WiseFs64.sys of the component IoControlCode Handler. The manipulation leads to denial of service. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The identifier VDB-222361 was assigned to this vulnerability.	3.3	More Details
CVE-2023-0196	NVIDIA CUDA Toolkit SDK contains a bug in cuobjdump, where a local user running the tool against an ill-formed binary may cause a null- pointer dereference, which may result in a limited denial of service.	3.3	More Details
CVE-2023-25169	discourse-yearly-review is a discourse plugin which publishes an automated Year in Review topic. In affected versions a user present in a yearly review topic that is then anonymised will still have some data linked to its original account. This issue has been patched in commit `b3ab33bbf7` which is included in the latest version of the Discourse Yearly Review plugin. Users are advised to upgrade. Users unable to upgrade may disable the `yearly_review_enabled` setting to fully mitigate the issue. Also, it's possible to edit the anonymised user's old data in the yearly review topics manually.	3.1	More Details
CVE-2023-1157	A vulnerability, which was classified as problematic, was found in finixbit elf-parser. Affected is the function elf_parser::Elf_parser::get_segments of the file elf_parser.cpp. The manipulation leads to denial of service. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. VDB-222222 is the identifier assigned to this vulnerability.	2.8	More Details
CVE-2022-4134	A flaw was found in openstack-glance. This issue could allow a remote, authenticated attacker to tamper with images, compromising the integrity of virtual machines created using these modified images.	2.8	More Details
CVE-2015-10093	A vulnerability was found in Mark User as Spammer Plugin 1.0.0/1.0.1 on WordPress. It has been declared as problematic. Affected by this vulnerability is the function user_row_actions of the file plugin/plugin.php. The manipulation of the argument url leads to cross site scripting. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. Upgrading to version 1.0.2 is able to address this issue. The identifier of the patch is e7059727274d2767c240c55c02c163eaa4ba6c62. It is recommended to upgrade the affected component. The identifier VDB-222325 was assigned to this vulnerability.	2.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1113	A vulnerability was found in SourceCodester Simple Payroll System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file admin/?page=admin of the component POST Parameter Handler. The manipulation of the argument fullname leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-222073 was assigned to this vulnerability.	2.4	More Details
CVE-2015-10094	A vulnerability was found in Fastly Plugin up to 0.97 on WordPress. It has been rated as problematic. Affected by this issue is the function post of the file lib/api.php. The manipulation of the argument url leads to cross site scripting. The attack may be launched remotely. Upgrading to version 0.98 is able to address this issue. The patch is identified as d7fe42538f4d4af500e3af9678b6b06fba731656. It is recommended to upgrade the affected component. VDB-222326 is the identifier assigned to this vulnerability.	2.4	More Details
CVE-2022-38735	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-2022-26339	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2022.	N/A	More Details
CVE-2022-26416	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2022.	N/A	More Details
CVE-2022-38737	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-2022-26347	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2022.	N/A	More Details
CVE-2023-1103	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was a duplicate of CVE-2022-4821. Notes: none.	N/A	More Details
CVE-2022-38738	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-2022-38736	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-2022-26031	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2022.	N/A	More Details
CVE-2022-26123	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2022.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26087	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2022.	N/A	More Details
CVE-2023-26823	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2023-0783. Reason: This record is a duplicate of CVE-2023-0783. Notes: All CVE users should reference CVE-2023-0783 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2021-23220	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2021.	N/A	More Details
CVE-2021-23224	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2021.	N/A	More Details
CVE-2021-23232	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2021.	N/A	More Details
CVE-2021-26246	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2021.	N/A	More Details
CVE-2022-21224	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2022.	N/A	More Details
CVE-2022-25889	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2022.	N/A	More Details
CVE-2022-25920	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2022.	N/A	More Details
CVE-2022-25957	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2022.	N/A	More Details
CVE-2022-25968	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2022.	N/A	More Details
CVE-2022-25997	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2022.	N/A	More Details
CVE-2022-26027	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2022.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23212	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2021.	N/A	More Details
CVE-2022-26039	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2022.	N/A	More Details
CVE-2022-26053	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2022.	N/A	More Details
CVE-2022-26055	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2022.	N/A	More Details
CVE-2022-26058	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2022.	N/A	More Details
CVE-2022-38739	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-2018-3673	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2021-23199	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2021.	N/A	More Details
CVE-2018-3644	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3648	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3651	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3653	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3654	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-3656	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3660	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3664	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3709	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3708	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3707	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3706	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3695	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3694	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3692	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3685	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3681	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3680	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-3678	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3677	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3676	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3675	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3647	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3642	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2021-23185	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2021.	N/A	More Details
CVE-2018-3637	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2022-38740	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-2022-38741	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-2022-3168	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-2022-40148	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-2022-42293	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 Number	Description	Base Score	Reference
CVE-2022-42294	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-2022-42295	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-2022-42296	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-2022-42297	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-2022-42298	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-25694	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-1247	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-2022-3857	Rejected reason: Maintainer contacted. This is a false-positive. The flaw does not actually exist and was erroneously tested.	N/A	More Details
CVE-2018-3674	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3614	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3618	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3622	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3623	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-3625	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3631	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2018-3636	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Details
CVE-2022-26418	Rejected reason: This candidate was in a CNA pool that was not assigned to any issues during 2022.	N/A	More Details