SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 09 November 2022

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 Number	Description	Base Score	Reference
CVE-2022-43546	A vulnerability has been identified in POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the EndTime-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device.	9.9	More Details
CVE-2022-43545	A vulnerability has been identified in POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the RecordType-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43439	A vulnerability has been identified in POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the Language-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device.	9.9	More Details
CVE-2022-3463	The Contact Form Plugin WordPress plugin before 4.3.13 does not validate and escape fields when exporting form entries as CSV, leading to a CSV injection	9.8	More Details
CVE-2022-44053	The d8s-networking for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code execution backdoor inserted by third parties is the democritus-user-agents package. The affected version of d8s-htm is 0.1.0.	9.8	More Details
CVE-2022-42920	Apache Commons BCEL has a number of APIs that would normally only allow changing specific class characteristics. However, due to an out-of-bounds writing issue, these APIs can be used to produce arbitrary bytecode. This could be abused in applications that pass attacker-controllable data to those APIs, giving the attacker more control over the resulting bytecode than otherwise expected. Update to Apache Commons BCEL 6.6.0.	9.8	More Details
CVE-2022-43303	The d8s-strings for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code execution backdoor inserted by third parties is the democritus-uuids package. The affected version of d8s-htm is 0.1.0.	9.8	More Details
CVE-2022-43304	The d8s-timer for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code execution backdoor inserted by third parties is the democritus-uuids package. The affected version of d8s-htm is 0.1.0.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43305	The d8s-python for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code execution backdoor inserted by third parties is the democritus-algorithms package. The affected version of d8s-htm is 0.1.0.	9.8	More Details
CVE-2022-44048	The d8s-urls for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code execution backdoor inserted by third parties is the democritus-domains package. The affected version of d8s-htm is 0.1.0.	9.8	More Details
CVE-2022-44049	The d8s-python for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code execution backdoor inserted by third parties is the democritus-grammars package. The affected version of d8s-htm is 0.1.0.	9.8	More Details
CVE-2022-44050	The d8s-networking for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code execution backdoor inserted by third parties is the democritus-json package. The affected version of d8s-htm is 0.1.0.	9.8	More Details
CVE-2022-44051	The d8s-stats for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code execution backdoor inserted by third parties is the democritus-math package. The affected version of d8s-htm is 0.1.0.	9.8	More Details
CVE-2022-44052	The d8s-dates for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code execution backdoor inserted by third parties is the democritus-timezones package. The affected version of d8s-htm is 0.1.0.	9.8	More Details
CVE-2022-31199	Remote code execution vulnerabilities exist in the Netwrix Auditor User Activity Video Recording component affecting both the Netwrix Auditor server and agents installed on monitored systems. The remote code execution vulnerabilities exist within the underlying protocol used by the component, and potentially allow an unauthenticated remote attacker to execute arbitrary code as the NT AUTHORITY\SYSTEM user on affected systems, including on systems Netwrix Auditor monitors.	9.8	More Details
CVE-2022-44054	The d8s-xml for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code execution backdoor inserted by third parties is the democritus-utility package. The affected version of d8s-htm is 0.1.0.	9.8	More Details
CVE-2022-3575	Frauscher Sensortechnik GmbH FDS102 for FAdC R2 and FAdCi R2 v2.8.0 to v2.9.1 are vulnerable to malicious code upload without authentication by using the configuration upload function. This could lead to a complete compromise of the FDS102 device.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44457	A vulnerability has been identified in Mendix SAML (Mendix 7 compatible) (All versions < V1.17.0), Mendix SAML (Mendix 7 compatible) (All versions >= V1.17.0 < V1.17.2), Mendix SAML (Mendix 8 compatible) (All versions < V2.3.0), Mendix SAML (Mendix 8 compatible) (All versions >= V2.3.0 < V2.3.2), Mendix SAML (Mendix 9 compatible, New Track) (All versions < V3.3.1), Mendix SAML (Mendix 9 compatible, New Track) (All versions >= V3.3.1 < V3.3.5), Mendix SAML (Mendix 9 compatible, Upgrade Track) (All versions < V3.3.0), Mendix SAML (Mendix 9 compatible, Upgrade Track) (All versions >= V3.3.0 < V3.3.4). Affected versions of the module insufficiently protect from packet capture replay, only when the not recommended, non default configuration option `'Allow Idp Initiated Authentication'` is enabled. This CVE entry describes the incomplete fix for CVE-2022-37011 in a specific non default configuration.	9.8	More Details
CVE-2022-33321	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	9.8	More Details
CVE-2022-27510	Unauthorized access to Gateway user capabilities	9.8	More Details
CVE-2022-34822	Path traversal vulnerability in CLUSTERPRO X 5.0 for Windows and earlier, EXPRESSCLUSTER X 5.0 for Windows and earlier, CLUSTERPRO X 5.0 SingleServerSafe for Windows and earlier, EXPRESSCLUSTER X 5.0 SingleServerSafe for Windows and earlier allows a remote unauthenticated attacker to overwrite existing files on the file system and to potentially execute arbitrary code.	9.8	More Details
CVE-2022-34823	Buffer overflow vulnerability in CLUSTERPRO X 5.0 for Windows and earlier, EXPRESSCLUSTER X 5.0 for Windows and earlier, CLUSTERPRO X 5.0 SingleServerSafe for Windows and earlier, EXPRESSCLUSTER X 5.0 SingleServerSafe for Windows and earlier allows a remote unauthenticated attacker to overwrite existing files on the file system and to potentially execute arbitrary code.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34824	Weak File and Folder Permissions vulnerability in CLUSTERPRO X 5.0 for Windows and earlier, EXPRESSCLUSTER X 5.0 for Windows and earlier, CLUSTERPRO X 5.0 SingleServerSafe for Windows and earlier, EXPRESSCLUSTER X 5.0 SingleServerSafe for Windows and earlier allows a remote unauthenticated attacker to overwrite existing files on the file system and to potentially execute arbitrary code.	9.8	More Details
CVE-2022-34825	Uncontrolled Search Path Element in CLUSTERPRO X 5.0 for Windows and earlier, EXPRESSCLUSTER X 5.0 for Windows and earlier, CLUSTERPRO X 5.0 SingleServerSafe for Windows and earlier, EXPRESSCLUSTER X 5.0 SingleServerSafe for Windows and earlier allows a remote unauthenticated attacker to overwrite existing files on the file system and to potentially execute arbitrary code.	9.8	More Details
CVE-2022-37015	Symantec Endpoint Detection and Response (SEDR) Appliance, prior to 4.7.0, may be susceptible to a privilege escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user.	9.8	More Details
CVE-2022-3481	The WooCommerce Dropshipping WordPress plugin before 4.4 does not properly sanitise and escape a parameter before using it in a SQL statement via a REST endpoint available to unauthenticated users, leading to a SQL injection	9.8	More Details
CVE-2022-39328	Grafana is an open-source platform for monitoring and observability. Versions starting with 9.2.0 and less than 9.2.4 contain a race condition in the authentication middlewares logic which may allow an unauthenticated user to query an administration endpoint under heavy load. This issue is patched in 9.2.4. There are no known workarounds.	9.8	More Details
CVE-2022-44797	btcd before 0.23.2, as used in Lightning Labs lnd before 0.15.2-beta and other Bitcoin-related products, mishandles witness size checking.	9.8	More Details
CVE-2020-22819	MKCMS V6.2 has SQL injection via the /ucenter/active.php verify parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39382	Keystone is a headless CMS for Node.js — built with GraphQL and React.`@keystone-6/core@3.0.0 ll 3.0.1` users that use `NODE_ENV` to trigger security-sensitive functionality in their production builds are vulnerable to `NODE_ENV` being inlined to `"development"` for user code, irrespective of what your environment variables. If you do not use `NODE_ENV` in your user code to trigger security-sensitive functionality, you are not impacted by this vulnerability. Any dependencies that use `NODE_ENV` to trigger particular behaviors (optimizations, security or otherwise) should still respect your environment's configured `NODE_ENV` variable. The application's dependencies, as found in `node_modules` (including `@keystone-6/core`), are typically not compiled as part of this process, and thus should be unaffected. We have tested this assumption by verifying that `NODE_ENV=production yarn keystone start` still uses secure cookies when using `statelessSessions`. This vulnerability has been fixed in @keystone-6/core@3.0.2, regression tests have been added for this vulnerability in #8063.	9.8	More Details
CVE-2022-43101	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the devName parameter in the formSetDeviceName function.	9.8	More Details
CVE-2022-43102	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the timeZone parameter in the fromSetSysTime function.	9.8	More Details
CVE-2022-43103	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the list parameter in the formSetQosBand function.	9.8	More Details
CVE-2022-43104	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the wpapsk_crypto parameter in the fromSetWirelessRepeat function.	9.8	More Details
CVE-2022-43105	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the shareSpeed parameter in the fromSetWifiGusetBasic function.	9.8	More Details
CVE-2022-43106	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the schedStartTime parameter in the setSchedWifi function.	9.8	More Details
CVE-2022-43107	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the time parameter in the setSmartPowerManagement function.	9.8	More Details
CVE-2022-43108	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the firewallEn parameter in the formSetFirewallCfg function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43109	D-Link DIR-823G v1.0.2 was found to contain a command injection vulnerability in the function SetNetworkTomographySettings. This vulnerability allows attackers to execute arbitrary commands via a crafted packet.	9.8	More Details
CVE-2020-22818	MKCMS V6.2 has SQL injection via /ucenter/reg.php name parameter.	9.8	More Details
CVE-2020-22820	MKCMS V6.2 has SQL injection via the /ucenter/repass.php name parameter.	9.8	More Details
CVE-2022-44796	An issue was discovered in Object First Ootbi BETA build 1.0.7.712. The authorization service has a flow that allows getting access to the Web UI without knowing credentials. For signing, the JWT token uses a secret key that is generated through a function that doesn't produce cryptographically strong sequences. An attacker can predict these sequences and generate a JWT token. As a result, an attacker can get access to the Web UI. This is fixed in Object First Ootbi BETA build 1.0.13.1611.	9.8	More Details
CVE-2022-22425	"IBM InfoSphere Information Server 11.7 is potentially vulnerable to CSV Injection. A remote attacker could execute arbitrary commands on the system, caused by improper validation of csv file contents. IBM X-Force ID: 223598."	9.8	More Details
CVE-2022-42744	CandidATS version 3.0.0 allows an external attacker to perform CRUD operations on the application databases. This is possible because the application does not correctly validate the entriesPerPage parameter against SQLi attacks.	9.8	More Details
CVE-2022-3023	Use of Externally-Controlled Format String in GitHub repository pingcap/tidb prior to 6.4.0, 6.1.3.	9.8	More Details
CVE-2022-31691	Spring Tools 4 for Eclipse version 4.16.0 and below as well as VSCode extensions such as Spring Boot Tools, Concourse CI Pipeline Editor, Bosh Editor and Cloudfoundry Manifest YML Support version 1.39.0 and below all use Snakeyaml library for YAML editing support. This library allows for some special syntax in the YAML that under certain circumstances allows for potentially harmful remote code execution by the attacker.	9.8	More Details
CVE-2022-39344	Azure RTOS USBX is a USB host, device, and on-the-go (OTG) embedded stack, that is fully integrated with Azure RTOS ThreadX. Prior to version 6.1.12, the USB DFU UPLOAD functionality may be utilized to introduce a buffer overflow resulting in overwrite of memory contents. In particular cases this may allow an attacker to bypass security features or execute arbitrary code. The implementation of `ux_device_class_dfu_control_request` function prevents buffer overflow during handling of DFU UPLOAD command when current state is `UX_SYSTEM_DFU_STATE_DFU_IDLE`. This issue has been patched, please upgrade to version 6.1.12. As a workaround, add the `UPLOAD_LENGTH` check in all possible states.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44544	Mahara 21.04 before 21.04.7, 21.10 before 21.10.5, 22.04 before 22.04.3, and 22.10 before 22.10.0 potentially allow a PDF export to trigger a remote shell if the site is running on Ubuntu and the flag -dSAFER is not set with Ghostscript.	9.8	More Details
CVE-2022-39353	xmldom is a pure JavaScript W3C standard-based (XML DOM Level 2 Core) `DOMParser` and `XMLSerializer` module. xmldom parses XML that is not well-formed because it contains multiple top level elements, and adds all root nodes to the `childNodes` collection of the `Document`, without reporting any error or throwing. This breaks the assumption that there is only a single root node in the tree, which led to issuance of CVE-2022-39299 as it is a potential issue for dependents. Update to @xmldom/xmldom@~0.7.7, @xmldom/xmldom@~0.8.4 (dist-tag latest) or @xmldom/xmldom@>=0.9.0-beta.4 (dist-tag next). As a workaround, please one of the following approaches depending on your use case: instead of searching for elements in the whole DOM, only search in the `documentElement`or reject a document with a document that has more then 1 `childNode`.	9.4	More Details
CVE-2022-40747	"IBM InfoSphere Information Server 11.7 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 236584."	9.1	More Details
CVE-2022-38168	Broken Access Control in User Authentication in Avaya Scopia Pathfinder 10 and 20 PTS version 8.3.7.0.4 allows remote unauthenticated attackers to bypass the login page, access sensitive information, and reset user passwords via URL modification.	9.1	More Details
CVE-2022-39387	XWiki OIDC has various tools to manipulate OpenID Connect protocol in XWiki. Prior to version 1.29.1, even if a wiki has an OpenID provider configured through its xwiki.properties, it is possible to provide a third party provider its details through request parameters. One can then bypass the XWiki authentication altogether by specifying its own provider through the oidc.endpoint.* request parameters (or by using an XWiki-based OpenID provider with oidc.xwikiprovider. With the same approach, one could also provide a specific group mapping through oidc.groups.mapping that would make his user automatically part of the XWikiAdminGroup. This issue has been patched, please upgrade to 1.29.1. There is no workaround, an upgrade of the authenticator is required.	9.1	More Details
CVE-2022-42905	In wolfSSL before 5.5.2, if callback functions are enabled (via the WOLFSSL_CALLBACKS flag), then a malicious TLS 1.3 client or network attacker can trigger a buffer over-read on the heap of 5 bytes. (WOLFSSL_CALLBACKS is only intended for debugging.)	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37865	With Apache Ivy 2.4.0 an optional packaging attribute has been introduced that allows artifacts to be unpacked on the fly if they used pack200 or zip packaging. For artifacts using the "zip", "jar" or "war" packaging Ivy prior to 2.5.1 doesn't verify the target path when extracting the archive. An archive containing absolute paths or paths that try to traverse "upwards" using ".." sequences can then write files to any location on the local fie system that the user executing Ivy has write access to. Ivy users of version 2.4.0 to 2.5.0 should upgrade to Ivy 2.5.1.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-44724	The Handy Tip macro in Stiltsoft Handy Macros for Confluence Server/Data Center 3.x before 3.5.5 allows remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability.	8.9	More Details
CVE-2022-39356	Discourse is a platform for community discussion. Users who receive an invitation link that is not scoped to a single email address can enter any non-admin user's email and gain access to their account when accepting the invitation. All users should upgrade to the latest version. A workaround is temporarily disabling invitations with `SiteSetting.max_invites_per_day = 0` or scope them to individual email addresses.	8.9	More Details
CVE-2022-3852	The VR Calendar plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.3.3. This is due to missing or incorrect nonce validation on several functions. This makes it possible for unauthenticated attackers to delete, and modify calendars as well as the plugin settings, via forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2022-3776	The Restaurant Menu – Food Ordering System – Table Reservation plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.3.1. This is due to missing or incorrect nonce validation on several functions called via AJAX actions such as forms_action, set_option, & chosen_options to name a few . This makes it possible for unauthenticated attackers to perform a variety of administrative actions like modifying forms, via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2022-43306	The d8s-timer for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code execution backdoor inserted by third parties is the democritus-dates package. The affected version of d8s-htm is 0.1.0.	8.8	More Details
CVE-2022-43318	Human Resource Management System v1.0 was discovered to contain a SQL injection vulnerability via the stateedit parameter at /hrm/state.php.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3536	The Role Based Pricing for WooCommerce WordPress plugin before 1.6.3 does not have authorisation and proper CSRF checks, as well as does not validate path given via user input, allowing any authenticated users like subscriber to perform PHAR deserialization attacks when they can upload a file, and a suitable gadget chain is present on the blog	8.8	More Details
CVE-2022-3494	The Complianz WordPress plugin before 6.3.4, and Complianz Premium WordPress plugin before 6.3.6 allow a translators to inject arbitrary SQL through an unsanitized translation. SQL can be injected through an infected translation file, or by a user with a translator role through translation plugins such as Loco Translate or WPML.	8.8	More Details
CVE-2022-43226	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /odlms/?page=appointments/view_appointment.	8.8	More Details
CVE-2022-44794	An issue was discovered in Object First Ootbi BETA build 1.0.7.712. Management protocol has a flow which allows a remote attacker to execute arbitrary Bash code with root privileges. The command that sets the hostname doesn't validate input parameters. As a result, arbitrary data goes directly to the Bash interpreter. An attacker would need credentials to exploit this vulnerability. This is fixed in Object First Ootbi BETA build 1.0.13.1611.	8.8	More Details
CVE-2022-43570	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, an authenticated user can perform an extensible markup language (XML) external entity (XXE) injection via a custom View. The XXE injection causes Splunk Web to embed incorrect documents into an error.	8.8	More Details
CVE-2022-43568	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, a View allows for a Reflected Cross Site Scripting via JavaScript Object Notation (JSON) in a query parameter when output_mode=radio.	8.8	More Details
CVE-2022-43567	In Splunk Enterprise versions below 8.2.9, 8.1.12, and 9.0.2, an authenticated user can run arbitrary operating system commands remotely through the use of specially crafted requests to the mobile alerts feature in the Splunk Secure Gateway app.	8.8	More Details
CVE-2022-41757	An issue was discovered in the Arm Mali GPU Kernel Driver. A non-privileged user can make improper GPU processing operations to obtain write access to read-only memory, or obtain access to already freed memory. This affects Valhall r29p0 through r38p1 before r38p2, and r39p0 before r40p0.	8.8	More Details
CVE-2022-44638	In libpixman in Pixman before 0.42.2, there is an out-of-bounds write (aka heap-based buffer overflow) in rasterize_edges_8 due to an integer overflow in pixman_sample_floor_y.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20961	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 request forgery (CSRF) attack and perform arbitrary actions on an affected device. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform arbitrary actions on the affected device with the privileges of the target user.	8.8	More Details
CVE-2022-3537	The Role Based Pricing for WooCommerce WordPress plugin before 1.6.2 does not have authorisation and proper CSRF checks, and does not validate files to be uploaded, allowing any authenticated users like subscriber to upload arbitrary files, such as PHP	8.8	More Details
CVE-2022-43571	In Splunk Enterprise versions below 8.2.9, 8.1.12, and 9.0.2, an authenticated user can execute arbitrary code through the dashboard PDF generation component.	8.8	More Details
CVE-2022-42750	CandidATS version 3.0.0 allows an external attacker to steal the cookie of arbitrary users. This is possible because the application does not correctly validate the files uploaded by the user.	8.8	More Details
CVE-2022-41203	In some workflow of SAP BusinessObjects BI Platform (Central Management Console and BI LaunchPad), an authenticated attacker with low privileges can intercept a serialized object in the parameters and substitute with another malicious serialized object, which leads to deserialization of untrusted data vulnerability. This could highly compromise the Confidentiality, Integrity, and Availability of the system.	8.8	More Details
CVE-2022-42751	CandidATS version 3.0.0 allows an external attacker to elevate privileges in the application. This is possible because the application suffers from CSRF. This allows to persuade an administrator to create a new account with administrative permissions.	8.8	More Details
CVE-2022-30608	"IBM InfoSphere Information Server 11.7 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a "user that the website trusts. IBM X-Force ID: 227295.	8.8	More Details
CVE-2022-38374	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiADC 7.0.0 - 7.0.2 and 6.2.0 - 6.2.4 allows an attacker to execute unauthorized code or commands via the URL and User fields observed in the traffic and event logviews.	8.8	More Details
CVE-2022-41214	Due to insufficient input validation, SAP NetWeaver Application Server ABAP and ABAP Platform allows an attacker with high level privileges to use a remote enabled function to delete a file which is otherwise restricted. On successful exploitation an attacker can completely compromise the integrity and availability of the application.	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3872	An off-by-one read/write issue was found in the SDHCI device of QEMU. It occurs when reading/writing the Buffer Data Port Register in sdhci_read_dataport and sdhci_write_dataport, respectively, if data_count == block_size. A malicious guest could use this flaw to crash the QEMU process on the host, resulting in a denial of service condition.	8.6	More Details
CVE-2021-44862	Netskope client is impacted by a vulnerability where an authenticated, local attacker can view sensitive information stored in NSClient logs which should be restricted. The vulnerability exists because the sensitive information is not masked/scrubbed before writing in the logs. A malicious user can use the sensitive information to download data and impersonate another user.	8.4	More Details
CVE-2022-43451	OpenHarmony-v3.1.2 and prior versions had an Multiple path traversal vulnerability in appspawn and nwebspawn services. Local attackers can create arbitrary directories or escape application sandbox.If chained with other vulnerabilities it would allow an unprivileged process to gain full root privileges.	8.4	More Details
CVE-2022-24936	Out-of-Bounds error in GBL parser in Silicon Labs Gecko Bootloader version 4.0.1 and earlier allows attacker to overwrite flash Sign key and OTA decryption key via malicious bootloader upgrade.	8.3	More Details
CVE-2022-20958	A vulnerability in the web-based management interface of Cisco BroadWorks CommPilot application could allow an unauthenticated, remote attacker to perform a server-side request forgery (SSRF) attack on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web interface. A successful exploit could allow the attacker to obtain confidential information from the BroadWorks server and other device on the network. {{value}} ["%7b%7bvalue%7d%7d"])}]]	8.3	More Details
CVE-2022-38660	HCL XPages applications are susceptible to a Cross Site Request Forgery (CSRF) vulnerability. An unauthenticated attacker could exploit this vulnerability to perform actions in the application on behalf of the logged in user.	8.3	More Details
CVE-2022-27513	Remote desktop takeover via phishing	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33684	The Apache Pulsar C++ Client does not verify peer TLS certificates when making HTTPS calls for the OAuth2.0 Client Credential Flow, even when tlsAllowInsecureConnection is disabled via configuration. This vulnerability allows an attacker to perform a man in the middle attack and intercept and/or modify the GET request that is sent to the ClientCredentialFlow 'issuer url'. The intercepted credentials can be used to acquire authentication data from the OAuth2.0 server to then authenticate with an Apache Pulsar cluster. An attacker can only take advantage of this vulnerability by taking control of a machine 'between' the client and the server. The attacker must then actively manipulate traffic to perform the attack. The Apache Pulsar Python Client wraps the C++ client, so it is also vulnerable in the same way. This issue affects Apache Pulsar C++ Client and Python Client versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.3; 2.9.0 to 2.9.2; 2.10.0 to 2.10.1; 2.6.4 and earlier. Any users running affected versions of the C++ Client or the Python Client should rotate vulnerable OAuth2.0 credentials, including client_id and client_secret. 2.7 C++ and Python Client users should upgrade to 2.7.5 and rotate vulnerable OAuth2.0 credentials. 2.8 C++ and Python Client users should upgrade to 2.8.4 and rotate vulnerable OAuth2.0 credentials. 2.9 C++ and Python Client users should upgrade to 2.9.3 and rotate vulnerable OAuth2.0 credentials. 2.10 C++ and Python Client users should upgrade to 2.10.2 and rotate vulnerable OAuth2.0 credentials. 3.0 C++ users are unaffected and 3.0 Python Client users will be unaffected when it is released. Any users running the C++ and Python Client for 2.6 or less should upgrade to one of the above patched versions.	8.1	More Details
CVE-2021-37789	stb_image.h 2.27 has a heap-based buffer over in stbi__jpeg_load, leading to Information Disclosure or Denial of Service.	8.1	More Details
CVE-2022-43565	In Splunk Enterprise versions below 8.2.9 and 8.1.12, the way that the ‘tstats command handles Javascript Object Notation (JSON) lets an attacker bypass SPL safeguards for risky commands https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/SPLsafeguards . The vulnerability requires the attacker to phish the victim by tricking them into initiating a request within their browser.	8.1	More Details
CVE-2022-43563	In Splunk Enterprise versions below 8.2.9 and 8.1.12, the way that the rex search command handles field names lets an attacker bypass SPL safeguards for risky commands https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/SPLsafeguards . The vulnerability requires the attacker to phish the victim by tricking them into initiating a request within their browser. The attacker cannot exploit the vulnerability at will.	8.1	More Details
CVE-2022-44311	html2xhtml v1.3 was discovered to contain an Out-Of-Bounds read in the function static void elm_close(tree_node_t *nodo) at procesador.c. This vulnerability allows attackers to access sensitive files or cause a Denial of Service (DoS) via a crafted html file.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43569	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, an authenticated user can inject and store arbitrary scripts that can lead to persistent cross-site scripting (XSS) in the object name of a Data Model.	8.0	More Details
CVE-2022-38373	An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiDeceptor management interface 4.2.0, 4.1.0 through 4.1.1, 4.0.2 may allow an authenticated user to perform a cross site scripting (XSS) attack via sending requests with specially crafted lure resource ID.	8.0	More Details
CVE-2022-35851	An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiADC management interface 7.1.0 may allow a remote and authenticated attacker to trigger a stored cross site scripting (XSS) attack via configuring a specially crafted IP Address.	8.0	More Details
CVE-2022-39950	An improper neutralization of input during web page generation vulnerability [CWE-79] exists in FortiManager and FortiAnalyzer 6.0.0 all versions, 6.2.0 all versions, 6.4.0 through 6.4.8, and 7.0.0 through 7.0.4. Report templates may allow a low privilege level attacker to perform an XSS attack via posting a crafted CKeditor "protected" comment as described in CVE-2020-9281.	8.0	More Details
CVE-2022-3558	The Import and export users and customers WordPress plugin before 1.20.5 does not properly escape data when exporting it via CSV files.	8.0	More Details
CVE-2022-40284	A buffer overflow was discovered in NTFS-3G before 2022.10.3. Crafted metadata in an NTFS image can cause code execution. A local attacker can exploit this if the ntfs-3g binary is setuid root. A physically proximate attacker can exploit this if NTFS-3G software is configured to execute upon attachment of an external storage device.	7.8	More Details
CVE-2022-37710	Patterson Dental Eaglesoft 21 has AES-256 encryption but there are two ways to obtain a keyfile: (1) keybackup.data > License > Encryption Key or (2) Eaglesoft.Server.Configuration.data > DbEncryptKeyPrimary > Encryption Key. Applicable files are encrypted with keys and salt that are hardcoded into a DLL or EXE file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42919	Python 3.9.x before 3.9.16 and 3.10.x before 3.10.9 on Linux allows local privilege escalation in a non-default configuration. The Python multiprocessing library, when used with the forkserver start method on Linux, allows pickles to be deserialized from any user in the same machine local network namespace, which in many system configurations means any user on the same machine. Pickles can execute arbitrary code. Thus, this allows for local user privilege escalation to the user that any forkserver process is running as. Setting multiprocessing.util.abstract_sockets_supported to False is a workaround. The forkserver start method for multiprocessing is not the default start method. This issue is Linux specific because only Linux supports abstract namespace sockets. CPython before 3.9 does not make use of Linux abstract namespace sockets by default. Support for users manually specifying an abstract namespace socket was added as a bugfix in 3.7.8 and 3.8.3, but users would need to make specific uncommon API calls in order to do that in CPython before 3.9.	7.8	More Details
CVE-2022-35717	"IBM InfoSphere Information Server 11.7 could allow a locally authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-"Force ID: 231361.	7.8	More Details
CVE-2021-34055	jhead 3.06 is vulnerable to Buffer Overflow via exif.c in function Put16u.	7.8	More Details
CVE-2022-26119	A improper authentication vulnerability in Fortinet FortiSIEM before 6.5.0 allows a local attacker with CLI access to perform operations on the Glassfish server directly via a hardcoded password.	7.8	More Details
CVE-2022-20452	In initializeFromParcelLocked of BaseBundle.java, there is a possible method arbitrary code execution due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-240138318	7.8	More Details
CVE-2022-41660	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.2 (All versions < V13.2.0.12), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected products contain an out of bounds write vulnerability when parsing a CGM file. An attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2022-32601	In telephony, there is a possible permission bypass due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319132; Issue ID: ALPS07319132.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20441	In navigateUpTo of Task.java, there is a possible way to launch an unexported intent handler due to a logic error in the code. This could lead to local escalation of privilege if the targeted app has an intent trampoline, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-238605611	7.8	More Details
CVE-2022-20450	In restorePermissionState of PermissionManagerServiceImpl.java, there is a possible way to bypass user consent due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-210065877	7.8	More Details
CVE-2022-43397	A vulnerability has been identified in Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.170), Simcenter Femap (All versions < V2023.1). The affected application contains an out of bounds write past the end of an allocated buffer while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17854)	7.8	More Details
CVE-2022-41664	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.2 (All versions < V13.2.0.12), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected application contains a stack-based buffer overflow vulnerability that could be triggered while parsing specially crafted PDF files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2022-41663	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.2 (All versions < V13.2.0.12), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected applications contain a use-after-free vulnerability that could be triggered while parsing specially crafted CGM files. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2022-41662	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.2 (All versions < V13.2.0.12), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected products contain an out of bounds read vulnerability when parsing a CGM file. An attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2022-20451	In onCallRedirectionComplete of CallsManager.java, there is a possible permissions bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-235098883	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39661	In _PMRLogicalOffsetToPhysicalOffset of the PowerVR kernel driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-246824784	7.8	More Details
CVE-2022-41661	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.2 (All versions < V13.2.0.12), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected products contain an out of bounds read vulnerability when parsing a CGM file. An attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2021-1050	In MMU_UnmapPages of the PowerVR kernel driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-243825200	7.8	More Details
CVE-2022-39157	A vulnerability has been identified in Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.0 (All versions >= V34.0.252 < V34.0.254), Parasolid V34.1 (All versions < V34.1.242), Parasolid V34.1 (All versions >= V34.1.242 < V34.1.244), Parasolid V35.0 (All versions < V35.0.170), Parasolid V35.0 (All versions >= V35.0.170 < V35.0.184), Simcenter Femap (All versions < V2023.1). The affected application contains an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17745)	7.8	More Details
CVE-2022-39136	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.2 (All versions < V13.2.0.12), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V13.3 (All versions >= V13.3.0.7 < V13.3.0.8), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected application is vulnerable to fixed-length heap-based buffer while parsing specially crafted TIF files. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2022-43359	Gifdec commit 1dcbae19363597314f6623010cc80abad4e47f7c was discovered to contain an out-of-bounds read in the function read_image_data. This vulnerability is triggered when parsing a crafted Gif file.	7.8	More Details
CVE-2022-44747	Local privilege escalation due to improper soft link handling. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 40107.	7.8	More Details
CVE-2022-20462	In phNxpNciHal_write_unlocked of phNxpNciHal.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-230356196	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44733	Local privilege escalation due to insecure folder permissions. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 39900.	7.8	More Details
CVE-2022-44732	Local privilege escalation due to insecure folder permissions. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 39900.	7.8	More Details
CVE-2022-33870	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the command line interpreter of FortiTester 3.0.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands.	7.8	More Details
CVE-2022-20951	A vulnerability in the web-based management interface of Cisco BroadWorks CommPilot application could allow an authenticated, remote attacker to perform a server-side request forgery (SSRF) attack on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web interface. A successful exploit could allow the attacker to obtain confidential information from the BroadWorks server and other device on the network. {{value}} ["%7b%7bvalue%7d%7d"])}]]	7.7	More Details
CVE-2021-45447	Hitachi Vantara Pentaho Business Analytics Server versions before 9.3.0.0, 9.2.0.2 and 8.3.0.25 with the Data Lineage feature enabled transmits database passwords in clear text. The transmission of sensitive data in clear text allows unauthorized actors with access to the network to sniff and obtain sensitive information that can be later used to gain unauthorized access.	7.7	More Details
CVE-2022-39241	Discourse is a platform for community discussion. A malicious admin could use this vulnerability to perform port enumeration on the local host or other hosts on the internal network, as well as against hosts on the Internet. Latest `stable`, `beta`, and `test-passed` versions are now patched. As a workaround, self-hosters can use `DISCOURSE_BLOCKED_IP_BLOCKS` env var (which overrides `blocked_ip_blocks` setting) to stop webhooks from accessing private IPs.	7.6	More Details
CVE-2022-43958	A vulnerability has been identified in QMS Automotive (All versions < V12.39), QMS Automotive (All versions < V12.39). User credentials are stored in plaintext in the database without any hashing mechanism. This could allow an attacker to gain access to credentials and impersonate other users.	7.6	More Details
CVE-2022-42745	CandidATS version 3.0.0 allows an external attacker to read arbitrary files from the server. This is possible because the application is vulnerable to XXE.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43574	"IBM Robotic Process Automation 21.0.1, 21.0.2, 21.0.3, 21.0.4, and 21.0.5 is vulnerable to incorrect permission assignment which could allow access to application configurations. IBM X-Force ID: 238679."	7.5	More Details
CVE-2022-20445	In process_service_search_rsp of sdp_discovery.cc, there is a possible out of bounds read due to improper input validation. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-225876506	7.5	More Details
CVE-2022-39386	@fastify/websocket provides WebSocket support for Fastify. Any application using @fastify/websocket could crash if a specific, malformed packet is sent. All versions of fastify-websocket are also impacted. That module is deprecated, so it will not be patched. This has been patched in version 7.1.1 (fastify v4) and version 5.0.1 (fastify v3). There are currently no known workarounds. However, it should be possible to attach the error handler manually. The recommended path is upgrading to the patched versions.	7.5	More Details
CVE-2022-43398	A vulnerability has been identified in POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50). Affected devices do not renew the session cookie after login/logout and also accept user defined session cookies. An attacker could overwrite the stored session cookie of a user. After the victim logged in, the attacker is given access to the user's account through the activated session.	7.5	More Details
CVE-2022-20960	A vulnerability in Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper handling of certain TLS connections that are processed by an affected device. An attacker could exploit this vulnerability by establishing a large number of concurrent TLS connections to an affected device. A successful exploit could allow the attacker to cause the device to drop new TLS email messages that come from the associated email servers. Exploitation of this vulnerability does not cause the affected device to unexpectedly reload. The device will recover autonomously within a few hours of when the attack is halted or mitigated.	7.5	More Details
CVE-2022-26446	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118.	7.5	More Details
CVE-2022-44556	Missing parameter type validation in the DRM module. Successful exploitation of this vulnerability may affect availability.	7.5	More Details
CVE-2022-43343	N-Prolog v1.91 was discovered to contain a global buffer overflow vulnerability in the function gettoken() at Main.c.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42955	The PassWork extension 5.0.9 for Chrome and other browsers allows an attacker to obtain cleartext cached credentials.	7.5	More Details
CVE-2022-43572	In Splunk Enterprise versions below 8.2.9, 8.1.12, and 9.0.2, sending a malformed file through the Splunk-to-Splunk (S2S) or HTTP Event Collector (HEC) protocols to an indexer results in a blockage or denial-of-service preventing further indexing.	7.5	More Details
CVE-2022-42707	In Mahara 21.04 before 21.04.7, 21.10 before 21.10.5, 22.04 before 22.04.3, and 22.10 before 22.10.0, embedded images are accessible without a sufficient permission check under certain conditions.	7.5	More Details
CVE-2020-12509	In s::can moni::tools in versions below 4.2 an unauthenticated attacker could get any file from the device by path traversal in the camera-file module.	7.5	More Details
CVE-2022-43319	An information disclosure vulnerability in the component vcs/downloadFiles.php?download=./search.php of Simple E-Learning System v1.0 allows attackers to read arbitrary files.	7.5	More Details
CVE-2022-42956	The PassWork extension 5.0.9 for Chrome and other browsers allows an attacker to obtain the cleartext master password.	7.5	More Details
CVE-2022-37866	When Apache Ivy downloads artifacts from a repository it stores them in the local file system based on a user-supplied "pattern" that may include placeholders for artifacts coordinates like the organisation, module or version. If said coordinates contain "../" sequences - which are valid characters for Ivy coordinates in general - it is possible the artifacts are stored outside of Ivy's local cache or repository or can overwrite different artifacts inside of the local cache. In order to exploit this vulnerability an attacker needs collaboration by the remote repository as Ivy will issue http requests containing ".." sequences and a "normal" repository will not interpret them as part of the artifact coordinates. Users of Apache Ivy 2.0.0 to 2.5.1 should upgrade to Ivy 2.5.1.	7.5	More Details
CVE-2022-43945	The Linux kernel NFSD implementation prior to versions 5.19.17 and 6.0.2 are vulnerable to buffer overflow. NFSD tracks the number of pages held by each NFSD thread by combining the receive and send buffers of a remote procedure call (RPC) into a single array of pages. A client can force the send buffer to shrink by sending an RPC message over TCP with garbage data added at the end of the message. The RPC message with garbage data is still correctly formed according to the specification and is passed forward to handlers. Vulnerable code in NFSD is not expecting the oversized request and writes beyond the allocated buffer space. CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39371	GLPI stands for Gestionnaire Libre de Parc Informatique. GLPI is a Free Asset and IT Management Software package that provides ITIL Service Desk features, licenses tracking and software auditing. Script related HTML tags in assets inventory information are not properly neutralized. This issue has been patched, please upgrade to version 10.0.4. There are currently no known workarounds.	7.5	More Details
CVE-2022-3181	An Improper Input Validation vulnerability exists in Trihedral VTScada version 12.0.38 and prior. A specifically malformed HTTP request could cause the affected VTScada to crash. Both local area network (LAN)-only and internet facing systems are affected.	7.5	More Details
CVE-2022-39381	Muhammara is a node module with c/cpp bindings to modify PDF with js for node or electron (based/replacement on/of galkhana/hummusjs). The package muhammara before 2.6.0; all versions of package hummus are vulnerable to Denial of Service (DoS) when supplied with a maliciously crafted PDF file to be appended to another. This issue has been patched in 2.6.0 for muhammara and not at all for hummus. As a workaround, do not process files from untrusted sources.	7.5	More Details
CVE-2022-32287	A relative path traversal vulnerability in a FileUtil class used by the PEAR management component of Apache UIMA allows an attacker to create files outside the designated target directory using carefully crafted ZIP entry names. This issue affects Apache UIMA Apache UIMA version 3.3.0 and prior versions. Note that PEAR files should never be installed into an UIMA installation from untrusted sources because PEAR archives are executable plugins that will be able to perform any actions with the same privileges as the host Java Virtual Machine.	7.5	More Details
CVE-2022-41716	Due to unsanitized NUL values, attackers may be able to maliciously set environment variables on Windows. In syscall.StartProcess and os/exec.Cmd, invalid environment variable values containing NUL values are not properly checked for. A malicious environment variable value can exploit this behavior to set a value for a different environment variable. For example, the environment variable string "A=B\x00C=D" sets the variables "A=B" and "C=D".	7.5	More Details
CVE-2022-27858	CSV Injection vulnerability in Activity Log Team Activity Log <= 2.8.3 on WordPress.	7.4	More Details
CVE-2022-39323	GLPI stands for Gestionnaire Libre de Parc Informatique. GLPI is a Free Asset and IT Management Software package that provides ITIL Service Desk features, licenses tracking and software auditing. Time based attack using a SQL injection in api REST user_token. This issue has been patched, please upgrade to version 10.0.4. As a workaround, disable login with user_token on API Rest.	7.4	More Details
CVE-2022-2904	A cross-site scripting issue has been discovered in GitLab CE/EE affecting all versions starting from 15.2 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1 It was possible to exploit a vulnerability in the external status checks feature which could lead to a stored XSS that allowed attackers to perform arbitrary actions on behalf of victims at client side.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43566	In Splunk Enterprise versions below 8.2.9, 8.1.12, and 9.0.2, an authenticated user can run risky commands using a more privileged user's permissions to bypass SPL safeguards for risky commands https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/SPLsafeguards in the Analytics Workspace. The vulnerability requires the attacker to phish the victim by tricking them into initiating a request within their browser. The attacker cannot exploit the vulnerability at will.	7.3	More Details
CVE-2022-44744	Local privilege escalation due to DLL hijacking vulnerability. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 40107.	7.3	More Details
CVE-2022-3878	A vulnerability classified as critical has been found in Maxon ERP. This affects an unknown part of the file /index.php/purchase_order/browse_data. The manipulation of the argument tb_search 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-213039.	7.3	More Details
CVE-2022-36077	The Electron framework enables writing cross-platform desktop applications using JavaScript, HTML and CSS. In versions prior to 21.0.0-beta.1, 20.0.1, 19.0.11, and 18.3.7, Electron is vulnerable to Exposure of Sensitive Information. When following a redirect, Electron delays a check for redirecting to file:// URLs from other schemes. The contents of the file is not available to the renderer following the redirect, but if the redirect target is a SMB URL such as `file://some.website.com/`, then in some cases, Windows will connect to that server and attempt NTLM authentication, which can include sending hashed credentials.This issue has been patched in versions: 21.0.0-beta.1, 20.0.1, 19.0.11, and 18.3.7. Users are recommended to upgrade to the latest stable version of Electron. If upgrading isn't possible, this issue can be addressed without upgrading by preventing redirects to file:// URLs in the `WebContents.on('will-redirect')` event, for all WebContents as a workaround.	7.2	More Details
CVE-2022-43061	Online Tours & Travels Management System v1.0 was discovered to contain an arbitrary file upload vulnerability in the component /operations/travellers.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details
CVE-2022-43049	Canteen Management System Project v1.0 was discovered to contain a SQL injection vulnerability via the component /youthappam/add-food.php.	7.2	More Details
CVE-2022-43063	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Users.php?f=delete_client.	7.2	More Details
CVE-2022-43052	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /odlms/classes/Users.php?f=delete.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43051	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /odlms/classes/Users.php?f=delete_test.	7.2	More Details
CVE-2022-43050	Online Tours & Travels Management System v1.0 was discovered to contain an arbitrary file upload vulnerability in the component update_profile.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details
CVE-2022-43350	Sanitization Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /php-sms/classes/Master.php?f=delete_inquiry.	7.2	More Details
CVE-2022-43062	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Master.php?f=delete_appointment.	7.2	More Details
CVE-2022-41551	Garage Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /garage/editorder.php.	7.2	More Details
CVE-2022-43352	Sanitization Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /php-sms/classes/Master.php?f=delete_quote.	7.2	More Details
CVE-2022-43066	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /odlms/classes/Master.php?f=delete_message.	7.2	More Details
CVE-2022-43068	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Master.php?f=delete_reservation.	7.2	More Details
CVE-2022-43227	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /odlms/admin/?page=appointments/view_appointment.	7.2	More Details
CVE-2022-2711	The Import any XML or CSV File to WordPress plugin before 3.6.9 is not validating the paths of files contained in uploaded zip archives, allowing highly privileged users, such as admins, to write arbitrary files to any part of the file system accessible by the web server via a path traversal vector.	7.2	More Details
CVE-2022-3418	The Import any XML or CSV File to WordPress plugin before 3.6.9 is not properly filtering which file extensions are allowed to be imported on the server, which could allow administrators in multi-site WordPress installations to upload arbitrary files	7.2	More Details
CVE-2022-42990	Food Ordering Management System v1.0 was discovered to contain a SQL injection vulnerability via the component /foms/all-orders.php?status=Cancelled%20by%20Customer.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20956	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to bypass authorization and access system files. This vulnerability is due to improper access control in the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to list, download, and delete certain files that they should not have access to. Cisco plans to release software updates that address this vulnerability. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-access-contol-EeufSUCx ["https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-access-contol-EeufSUCx"]	7.1	More Details
CVE-2021-45448	Pentaho Business Analytics Server versions before 9.2.0.2 and 8.3.0.25 using the Pentaho Analyzer plugin exposes a service endpoint for templates which allows a user-supplied path to access resources that are out of bounds. The software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory. By using special elements such as ".." and "/" separators, attackers can escape outside of the restricted location to access files or directories that are elsewhere on the system.	7.1	More Details
CVE-2022-43995	Sudo 1.8.0 through 1.9.12, with the crypt() password backend, contains a plugins/sudoers/auth/passwd.c array-out-of-bounds error that can result in a heap-based buffer over-read. This can be triggered by arbitrary local users with access to Sudo by entering a password of seven characters or fewer. The impact could vary depending on the system libraries, compiler, and processor architecture.	7.1	More Details
CVE-2022-41667	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that allows adversaries with local user privileges to load a malicious DLL which could lead to execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior).	7.0	More Details
CVE-2022-41669	A CWE-347: Improper Verification of Cryptographic Signature vulnerability exists in the SGIUtility component that allows adversaries with local user privileges to load a malicious DLL which could result in execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior).	7.0	More Details
CVE-2022-41670	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists in the SGIUtility component that allows adversaries with local user privileges to load malicious DLL which could result in execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior).	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41671	A CWE-89: Improper Neutralization of Special Elements used in SQL Command ('SQL Injection') vulnerability exists that allows adversaries with local user privileges to craft a malicious SQL query and execute as part of project migration which could result in execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior).	7.0	More Details
CVE-2022-41668	A CWE-704: Incorrect Project Conversion vulnerability exists that allows adversaries with local user privileges to load a project file from an adversary-controlled network share which could result in execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior).	7.0	More Details
CVE-2022-41666	A CWE-347: Improper Verification of Cryptographic Signature vulnerability exists that allows adversaries with local user privileges to load a malicious DLL which could lead to execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior).	7.0	More Details
CVE-2022-39377	sysstat is a set of system performance tools for the Linux operating system. On 32 bit systems, in versions 9.1.16 and newer but prior to 12.7.1, allocate_structures contains a size_t overflow in sa_common.c. The allocate_structures function insufficiently checks bounds before arithmetic multiplication, allowing for an overflow in the size allocated for the buffer representing system activities. This issue may lead to Remote Code Execution (RCE). This issue has been patched in version 12.7.1.	7.0	More Details
CVE-2022-41211	Due to lack of proper memory management, when a victim opens manipulated file received from untrusted sources in SAP 3D Visual Enterprise Author and SAP 3D Visual Enterprise Viewer, Arbitrary Code Execution can be triggered when payload forces:Re-use of dangling pointer which refers to overwritten space in memory. The accessed memory must be filled with code to execute the attack. Therefore, repeated success is unlikely.Stack-based buffer overflow. Since the memory overwritten is random, based on access rights of the memory, repeated success is not assured.	7.0	More Details
CVE-2022-32617	In typec, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07262364; Issue ID: ALPS07262364.	6.8	More Details
CVE-2022-32618	In typec, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07262454; Issue ID: ALPS07262454.	6.8	More Details
CVE-2022-32614	In audio, there is a possible memory corruption 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: ALPS07310571; Issue ID: ALPS07310571.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32603	In gpu drm, 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: ALPS07310704; Issue ID: ALPS07310704.	6.7	More Details
CVE-2022-32615	In ccd, there is a possible out of bounds write due to uninitialized data. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07326559; Issue ID: ALPS07326559.	6.7	More Details
CVE-2022-32616	In isp, there is a possible out of bounds write due to uninitialized data. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07341258; Issue ID: ALPS07341258.	6.7	More Details
CVE-2022-32611	In isp, 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: ALPS07340373; Issue ID: ALPS07340373.	6.7	More Details
CVE-2022-32605	In isp, 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: ALPS07213898; Issue ID: ALPS07213898.	6.7	More Details
CVE-2022-20454	In fdt_next_tag of fdt.c, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242096164	6.7	More Details
CVE-2022-38372	A hidden functionality vulnerability [CWE-1242] in FortiTester CLI 2.3.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow a local, privileged user to obtain a root shell on the device via an undocumented command.	6.7	More Details
CVE-2022-32607	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891.	6.7	More Details
CVE-2022-21778	In vpu, there is a possible information disclosure 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: ALPS06382421; Issue ID: ALPS06382421.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40263	BD Totalys MultiProcessor, versions 1.70 and earlier, contain hardcoded credentials. If exploited, threat actors may be able to access, modify or delete sensitive information, including electronic protected health information (ePHI), protected health information (PHI) and personally identifiable information (PII). Customers using BD Totalys MultiProcessor version 1.70 with Microsoft Windows 10 have additional operating system hardening configurations which increase the attack complexity required to exploit this vulnerability.	6.6	More Details
CVE-2022-34339	"IBM Cognos Analytics 11.2.1, 11.2.0, 11.1.7 stores user credentials in plain clear text which can be read by an authenticated user. IBM X-Force ID: 229963."	6.5	More Details
CVE-2022-38164	A vulnerability affecting F-Secure SAFE browser for Android and iOS was discovered. A maliciously crafted website could make a phishing attack with URL spoofing as the browser only display certain part of the entire URL.	6.5	More Details
CVE-2022-20942	A vulnerability in the web-based management interface of Cisco Email Security Appliance (ESA), Cisco Secure Email and Web Manager, and Cisco Secure Web Appliance, formerly known as Cisco Web Security Appliance (WSA), could allow an authenticated, remote attacker to retrieve sensitive information from an affected device, including user credentials. This vulnerability is due to weak enforcement of back-end authorization checks. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain confidential data that is stored on the affected device.	6.5	More Details
CVE-2022-43351	Sanitization Management System v1.0 was discovered to contain an arbitrary file deletion vulnerability via the component /classes/Master.php?f=delete_img.	6.5	More Details
CVE-2022-43238	Libde265 v1.0.8 was discovered to contain an unknown crash via ff_hevc_put_hevc_qpel_h_3_v_3_sse in sse-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file.	6.5	More Details
CVE-2022-43252	Libde265 v1.0.8 was discovered to contain a heap-buffer-overflow vulnerability via put_epel_16_fallback in fallback-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file.	6.5	More Details
CVE-2022-43253	Libde265 v1.0.8 was discovered to contain a heap-buffer-overflow vulnerability via put_unweighted_pred_16_fallback in fallback-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file.	6.5	More Details
CVE-2022-2188	Privilege escalation vulnerability in DXL Broker for Windows prior to 6.0.0.280 allows local users to gain elevated privileges by exploiting weak directory controls in the logs directory. This can lead to a denial-of-service attack on the DXL Broker.	6.5	More Details
CVE-2022-43249	Libde265 v1.0.8 was discovered to contain a heap-buffer-overflow vulnerability via put_epel_hv_fallback<unsigned short> in fallback-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22442	"IBM InfoSphere Information Server 11.7 could allow an authenticated user to access information restricted to users with elevated privileges due to improper access controls. IBM X-Force ID: 224427."	6.5	More Details
CVE-2022-20447	In PAN_WriteBuf of pan_api.cc, there is a possible out of bounds read due to a use after free. This could lead to remote information disclosure over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-233604485	6.5	More Details
CVE-2022-44795	An issue was discovered in Object First Ootbi BETA build 1.0.7.712. A flaw was found in the Web Service, which could lead to local information disclosure. The command that creates the URL for the support bundle uses an insecure RNG. That can lead to prediction of the generated URL. As a result, an attacker can get access to system logs. An attacker would need credentials to exploit this vulnerability. This is fixed in Object First Ootbi BETA build 1.0.13.1611. Important note - This vulnerability is related to the Object First Ootbi BETA version, which is not released for production and therefore has no impact on the production environment. The production-ready Object First Ootbi version will have this vulnerability fixed.	6.5	More Details
CVE-2022-44793	handle_ipv6IpForwarding in agent/mibgroup/ip-mib/ip_scalars.c in Net-SNMP 5.4.3 through 5.9.3 has a NULL Pointer Exception bug that can be used by a remote attacker to cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.	6.5	More Details
CVE-2022-41258	Due to insufficient input validation, SAP Financial Consolidation - version 1010, allows an authenticated attacker to inject malicious script when running a common query in the Web Administration Console. On successful exploitation, an attacker can view or modify information causing a limited impact on confidentiality, integrity and availability of the application.	6.5	More Details
CVE-2022-41259	SAP SQL Anywhere - version 17.0, allows an authenticated attacker to prevent legitimate users from accessing a SQL Anywhere database server by crashing the server with some queries that use an ARRAY constructor.	6.5	More Details
CVE-2022-43250	Libde265 v1.0.8 was discovered to contain a heap-buffer-overflow vulnerability via put_qpel_0_0_fallback_16 in fallback-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file.	6.5	More Details
CVE-2022-44792	handle_ipDefaultTTL in agent/mibgroup/ip-mib/ip_scalars.c in Net-SNMP 5.8 through 5.9.3 has a NULL Pointer Exception bug that can be used by a remote attacker (who has write access) to cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.	6.5	More Details
CVE-2022-43237	Libde265 v1.0.8 was discovered to contain a stack-buffer-overflow vulnerability via void put_epel_hv_fallback<unsigned short> in fallback-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file.	6.5	More Details
CVE-2022-43240	Libde265 v1.0.8 was discovered to contain a heap-buffer-overflow vulnerability via ff_hevc_put_hevc_qpel_h_2_v_1_sse in sse-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43241	Libde265 v1.0.8 was discovered to contain an unknown crash via ff_hevc_put_hevc_qpel_v_3_8_sse in sse-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file.	6.5	More Details
CVE-2022-44624	In JetBrains TeamCity version before 2022.10, Password parameters could be exposed in the build log if they contained special characters	6.5	More Details
CVE-2022-30694	The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack.	6.5	More Details
CVE-2022-43235	Libde265 v1.0.8 was discovered to contain a heap-buffer-overflow vulnerability via ff_hevc_put_hevc_epel_pixels_8_sse in sse-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file.	6.5	More Details
CVE-2022-43244	Libde265 v1.0.8 was discovered to contain a heap-buffer-overflow vulnerability via put_qpel_fallback<unsigned short> in fallback-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file.	6.5	More Details
CVE-2022-43495	OpenHarmony-v3.1.2 and prior versions had a DOS vulnerability in distributedhardware_device_manager when joining a network. Network attakcers can send an abonormal packet when joining a network, cause a nullptr reference and device reboot.	6.5	More Details
CVE-2022-44623	In JetBrains TeamCity version before 2022.10, Project Viewer could see scrambled secure values in the MetaRunner settings	6.5	More Details
CVE-2022-38582	Incorrect access control in the anti-virus driver wsdkd.sys of Watchdog Antivirus v1.4.158 allows attackers to write arbitrary files.	6.5	More Details
CVE-2022-43242	Libde265 v1.0.8 was discovered to contain a heap-buffer-overflow vulnerability via mc_luma<unsigned char> in motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file.	6.5	More Details
CVE-2022-43245	Libde265 v1.0.8 was discovered to contain a segmentation violation via apply_sao_internal<unsigned short> in sao.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file.	6.5	More Details
CVE-2022-43248	Libde265 v1.0.8 was discovered to contain a heap-buffer-overflow vulnerability via put_weighted_pred_avg_16_fallback in fallback-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file.	6.5	More Details
CVE-2022-40235	"IBM InfoSphere Information Server 11.7 could allow a user to cause a denial of service by removing the ability to run jobs due to improper input validation. IBM X-Force ID: 235725."	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43239	Libde265 v1.0.8 was discovered to contain a heap-buffer-overflow vulnerability via mc_chroma<unsigned short> in motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file.	6.5	More Details
CVE-2022-40230	"IBM MQ Appliance 9.2 CD, 9.2 LTS, 9.3 CD, and LTS 9.3 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 235532."	6.5	More Details
CVE-2022-43236	Libde265 v1.0.8 was discovered to contain a stack-buffer-overflow vulnerability via put_qpel_fallback<unsigned short> in fallback-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file.	6.5	More Details
CVE-2021-39432	diplib v3.0.0 is vulnerable to Double Free.	6.5	More Details
CVE-2022-43243	Libde265 v1.0.8 was discovered to contain a heap-buffer-overflow vulnerability via ff_hevc_put_weighted_pred_avg_8_sse in sse-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file.	6.5	More Details
CVE-2022-32609	In vcu, there is a possible use after 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: ALPS07203410; Issue ID: ALPS07203410.	6.4	More Details
CVE-2022-43561	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, a remote user that holds the “power” Splunk role can store arbitrary scripts that can lead to persistent cross-site scripting (XSS). The vulnerability affects instances with Splunk Web enabled.	6.4	More Details
CVE-2022-32608	In jpeg, there is a possible use after 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: ALPS07388753; Issue ID: ALPS07388753.	6.4	More Details
CVE-2022-32613	In vcu, there is a possible memory corruption 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: ALPS07206340; Issue ID: ALPS07206340.	6.4	More Details
CVE-2022-32612	In vcu, there is a possible use after 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: ALPS07203500; Issue ID: ALPS07203500.	6.4	More Details
CVE-2022-32610	In vcu, there is a possible use after 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: ALPS07203476; Issue ID: ALPS07203476.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3827	A vulnerability was found in centreon. It has been declared as critical. This vulnerability affects unknown code of the file formContactGroup.php of the component Contact Groups Form. The manipulation of the argument cg_id leads to sql injection. The attack can be initiated remotely. The name of the patch is 293b10628f7d9f83c6c82c78cf637cbe9b907369. It is recommended to apply a patch to fix this issue. VDB-212794 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-40206	Insecure direct object references (IDOR) vulnerability in the wpForo Forum plugin <= 2.0.5 on WordPress allows attackers with subscriber or higher user roles to mark any forum post as private/public.	6.3	More Details
CVE-2022-3825	A vulnerability was found in Huaxia ERP 2.3 and classified as critical. Affected by this issue is some unknown functionality of the component User Management. The manipulation of the argument login leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-212792.	6.3	More Details
CVE-2022-2696	The Restaurant Menu – Food Ordering System – Table Reservation plugin for WordPress is vulnerable to authorization bypass via several AJAX actions in versions up to, and including 2.3.0 due to missing capability checks and missing nonce validation. This makes it possible for authenticated attackers with minimal permissions to perform a wide variety of actions such as modifying the plugin's settings and modifying the ordering system preferences.	6.3	More Details
CVE-2022-43449	OpenHarmony-v3.1.2 and prior versions had an Arbitrary file read vulnerability via download_server. Local attackers can install an malicious application on the device and reveal any file from the filesystem that is accessible to download_server service which run with UID 1000.	6.2	More Details
CVE-2022-33322	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	6.1	More Details
CVE-2022-43982	In Apache Airflow versions prior to 2.4.2, the "Trigger DAG with config" screen was susceptible to XSS attacks via the `origin` query argument.	6.1	More Details
CVE-2022-42749	CandidATS version 3.0.0 on 'page' of the 'ajax.php' resource, allows an external attacker to steal the cookie of arbitrary users. This is possible because the application application does not properly validate user input against XSS attacks.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42746	CandidATS version 3.0.0 on 'indexFile' of the 'ajax.php' resource, allows an external attacker to steal the cookie of arbitrary users. This is possible because the application application does not properly validate user input against XSS attacks.	6.1	More Details
CVE-2022-40840	ndk design NdkAdvancedCustomizationFields 3.5.0 is vulnerable to Cross Site Scripting (XSS) via createPdf.php.	6.1	More Details
CVE-2022-41434	EyesOfNetwork Web Interface v5.3 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the component /lilac/main.php.	6.1	More Details
CVE-2022-27914	An issue was discovered in Joomla! 4.0.0 through 4.2.4. Inadequate filtering of potentially malicious user input leads to reflected XSS vulnerabilities in com_media.	6.1	More Details
CVE-2022-41136	Cross-Site Request Forgery (CSRF) vulnerability leading to Stored Cross-Site Scripting (XSS) in Vladimir Anokhin's Shortcodes Ultimate plugin <= 5.12.0 on WordPress.	6.1	More Details
CVE-2022-44741	Cross-Site Request Forgery (CSRF) vulnerability leading to Cross-Site Scripting (XSS) in David Anderson Testimonial Slider plugin <= 1.3.1 on WordPress.	6.1	More Details
CVE-2022-42747	CandidATS version 3.0.0 on 'sortBy' of the 'ajax.php' resource, allows an external attacker to steal the cookie of arbitrary users. This is possible because the application application does not properly validate user input against XSS attacks.	6.1	More Details
CVE-2022-43317	A cross-site scripting (XSS) vulnerability in /hrm/index.php?msg of Human Resource Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	6.1	More Details
CVE-2022-43985	In Apache Airflow versions prior to 2.4.2, there was an open redirect in the webserver's `/confirm` endpoint.	6.1	More Details
CVE-2022-3873	Cross-site Scripting (XSS) - DOM in GitHub repository jgraph/drawio prior to 20.5.2.	6.1	More Details
CVE-2022-42748	CandidATS version 3.0.0 on 'sortDirection' of the 'ajax.php' resource, allows an external attacker to steal the cookie of arbitrary users. This is possible because the application application does not properly validate user input against XSS attacks.	6.1	More Details
CVE-2022-3869	Code Injection in GitHub repository froxlor/froxlor prior to 0.10.38.2.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41260	SAP Financial Consolidation - version 1010, does not sufficiently encode user-controlled input which may allow an unauthenticated attacker to inject a web script via a GET request. On successful exploitation, an attacker can view or modify information causing a limited impact on confidentiality and integrity of the application.	6.1	More Details
CVE-2022-41207	SAP Biller Direct allows an unauthenticated attacker to craft a legitimate looking URL. When clicked by an unsuspecting victim, it will use an unsensitized parameter to redirect the victim to a malicious site of the attacker's choosing which can result in disclosure or modification of the victim's information.	6.1	More Details
CVE-2022-42753	SalonERP version 3.0.2 allows an external attacker to steal the cookie of arbitrary users. This is possible because the application does not correctly validate the page parameter against XSS attacks.	6.1	More Details
CVE-2021-46853	Alpine before 2.25 allows remote attackers to cause a denial of service (application crash) when LIST or LSUB is sent before STARTTLS.	5.9	More Details
CVE-2022-3340	XML External Entity (XXE) vulnerability in Trellix IPS Manager prior to 10.1 M8 allows a remote authenticated administrator to perform XXE attack in the administrator interface part of the interface, which allows a saved XML configuration file to be imported.	5.9	More Details
CVE-2022-38712	"IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Web services could allow a man-in-the-middle attacker to conduct SOAPAction spoofing to execute unwanted or unauthorized operations. IBM X-Force ID: 234762."	5.9	More Details
CVE-2022-39343	Azure RTOS FileX is a FAT-compatible file system that’s fully integrated with Azure RTOS ThreadX. In versions before 6.2.0, the Fault Tolerant feature of Azure RTOS FileX includes integer under and overflows which may be exploited to achieve buffer overflow and modify memory contents. When a valid log file with correct ID and checksum is detected by the `_fx_fault_tolerant_enable` function an attempt to recover the previous failed write operation is taken by call of `_fx_fault_tolerant_apply_logs`. This function iterates through the log entries and performs required recovery operations. When properly crafted a log including entries of type `FX_FAULT_TOLERANT_DIR_LOG_TYPE` may be utilized to introduce unexpected behavior. This issue has been patched in version 6.2.0. A workaround to fix line 218 in fx_fault_tolerant_apply_logs.c is documented in the GHSA.	5.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39384	OpenZeppelin Contracts is a library for secure smart contract development. Before version 4.4.1 but after 3.2.0, initializer functions that are invoked separate from contract creation (the most prominent example being minimal proxies) may be reentered if they make an untrusted non-view external call. Once an initializer has finished running it can never be re-executed. However, an exception put in place to support multiple inheritance made reentrancy possible in the scenario described above, breaking the expectation that there is a single execution. Note that upgradeable proxies are commonly initialized together with contract creation, where reentrancy is not feasible, so the impact of this issue is believed to be minor. This issue has been patched, please upgrade to version 4.4.1. As a workaround, avoid untrusted external calls during initialization.	5.6	More Details
CVE-2022-44318	PicoC Version 3.2.2 was discovered to contain a heap buffer overflow in the StringStrcat function in cstdlib/string.c when called from ExpressionParseFunctionCall.	5.5	More Details
CVE-2022-44745	Sensitive information leak through log files. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 40107.	5.5	More Details
CVE-2022-44746	Sensitive information disclosure due to insecure folder permissions. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 40107.	5.5	More Details
CVE-2022-44321	PicoC Version 3.2.2 was discovered to contain a heap buffer overflow in the LexSkipComment function in lex.c when called from LexScanGetToken.	5.5	More Details
CVE-2022-44319	PicoC Version 3.2.2 was discovered to contain a heap buffer overflow in the StdioBasePrintf function in cstdlib/string.c when called from ExpressionParseFunctionCall.	5.5	More Details
CVE-2022-20426	In multiple functions of many files, there is a possible obstruction of the user's ability to select a phone account due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-236263294	5.5	More Details
CVE-2022-44317	PicoC Version 3.2.2 was discovered to contain a heap buffer overflow in the StdioOutPutc function in cstdlib/stdio.c when called from ExpressionParseFunctionCall.	5.5	More Details
CVE-2022-41205	SAP GUI allows an authenticated attacker to execute scripts in the local network. On successful exploitation, the attacker can gain access to registries which can cause a limited impact on confidentiality and high impact on availability of the application.	5.5	More Details
CVE-2022-44316	PicoC Version 3.2.2 was discovered to contain a heap buffer overflow in the LexGetStringConstant function in lex.c when called from LexScanGetToken.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44315	PicoC Version 3.2.2 was discovered to contain a heap buffer overflow in the ExpressionAssign function in expression.c when called from ExpressionParseFunctionCall.	5.5	More Details
CVE-2022-44314	PicoC Version 3.2.2 was discovered to contain a heap buffer overflow in the StringStrncpy function in cstdlib/string.c when called from ExpressionParseFunctionCall.	5.5	More Details
CVE-2022-44313	PicoC Version 3.2.2 was discovered to contain a heap buffer overflow in the ExpressionCoerceUnsignedInteger function in expression.c when called from ExpressionParseFunctionCall.	5.5	More Details
CVE-2022-44312	PicoC Version 3.2.2 was discovered to contain a heap buffer overflow in the ExpressionCoerceInteger function in expression.c when called from ExpressionInfixOperator.	5.5	More Details
CVE-2022-3821	An off-by-one Error issue was discovered in Systemd in format_timespan() function of time-util.c. An attacker could supply specific values for time and accuracy that leads to buffer overrun in format_timespan(), leading to a Denial of Service.	5.5	More Details
CVE-2022-44320	PicoC Version 3.2.2 was discovered to contain a heap buffer overflow in the ExpressionCoerceFP function in expression.c when called from ExpressionParseFunctionCall.	5.5	More Details
CVE-2022-38654	HCL Domino is susceptible to an information disclosure vulnerability. In some scenarios, local calls made on the server to search the Domino directory will ignore xACL read restrictions. An authenticated attacker could leverage this vulnerability to access attributes from a user's person record.	5.5	More Details
CVE-2022-20414	In setImpl of AlarmManagerService.java, there is a possible way to put a device into a boot loop due to an uncaught exception. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-234441463	5.5	More Details
CVE-2022-20457	In getMountModeInternal of StorageManagerService.java, there is a possible prevention of package installation due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-243924784	5.5	More Details
CVE-2022-20448	In buzzBeepBlinkLocked of NotificationManagerService.java, there is a possible way to share data across users due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-237540408	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20453	In update of MmsProvider.java, there is a possible constriction of directory permissions due to a path traversal error. This could lead to local denial of service of SIM recognition with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-240685104	5.5	More Details
CVE-2022-41710	Markdownify version 1.4.1 allows an external attacker to remotely obtain arbitrary local files on any client that attempts to view a malicious markdown file through Markdownify. This is possible because the application does not have a CSP policy (or at least not strict enough) and/or does not properly validate the contents of markdown files before rendering them.	5.5	More Details
CVE-2022-32602	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07388790; Issue ID: ALPS07388790.	5.5	More Details
CVE-2022-40276	Zettlr version 2.3.0 allows an external attacker to remotely obtain arbitrary local files on any client that attempts to view a malicious markdown file through Zettlr. This is possible because the application does not have a CSP policy (or at least not strict enough) and/or does not properly validate the contents of markdown files before rendering them.	5.5	More Details
CVE-2022-43254	GPAC v2.1-DEV-rev368-gfd054169b-master was discovered to contain a memory leak via the component gf_list_new at utils/list.c.	5.5	More Details
CVE-2022-43255	GPAC v2.1-DEV-rev368-gfd054169b-master was discovered to contain a memory leak via the component gf_odf_new_iod at odf/odf_code.c.	5.5	More Details
CVE-2022-40223	Nonce token leakage and missing authorization in SearchWP premium plugin <= 4.2.5 on WordPress leading to plugin settings change.	5.4	More Details
CVE-2022-35642	"IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 227592."	5.4	More Details
CVE-2022-41208	Due to insufficient input validation, SAP Financial Consolidation - version 1010, allows an authenticated attacker with user privileges to alter current user session. On successful exploitation, the attacker can view or modify information, causing a limited impact on confidentiality and integrity of the application.	5.4	More Details
CVE-2022-43670	An improper neutralization of input during web page generation ('Cross-site Scripting') [CWE-79] vulnerability in Sling App CMS version 1.1.0 and prior may allow an authenticated remote attacker to perform a reflected cross site scripting (XSS) attack in the taxonomy management feature.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39945	An improper access control vulnerability [CWE-284] in FortiMail 7.2.0, 7.0.0 through 7.0.3, 6.4 all versions, 6.2 all versions, 6.0 all versions may allow an authenticated admin user assigned to a specific domain to access and modify other domains information via insecure direct object references (IDOR).	5.4	More Details
CVE-2022-30615	"IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 227592.	5.4	More Details
CVE-2022-40131	Cross-Site Request Forgery (CSRF) vulnerability in a3rev Software Page View Count plugin <= 2.5.5 on WordPress allows an attacker to reset the plugin settings.	5.4	More Details
CVE-2022-36404	Missing Authorization, Cross-Site Request Forgery (CSRF) vulnerability in David Cole Simple SEO (WordPress plugin) plugin <= 1.8.12 versions.	5.4	More Details
CVE-2022-32587	Cross-Site Request Forgery (CSRF) vulnerability in CodeAndMore WP Page Widget plugin <= 3.9 on WordPress leading to plugin settings change.	5.4	More Details
CVE-2021-40303	perfex crm 1.10 is vulnerable to Cross Site Scripting (XSS) via /clients/profile.	5.4	More Details
CVE-2022-27855	Cross-Site Request Forgery (CSRF) vulnerability in Fatcat Apps Analytics Cat plugin <= 1.0.9 on WordPress allows Plugin Settings Change.	5.4	More Details
CVE-2022-43491	Cross-Site Request Forgery (CSRF) vulnerability in Advanced Dynamic Pricing for WooCommerce plugin <= 4.1.5 on WordPress leading to plugin settings import.	5.4	More Details
CVE-2022-43481	Cross-Site Request Forgery (CSRF) vulnerability in Advanced Coupons for WooCommerce Coupons plugin <= 4.5 on WordPress leading to notice dismissal.	5.4	More Details
CVE-2022-40632	Cross-Site Request Forgery (CSRF) vulnerability in gVectors Team wpForo Forum plugin <= 2.0.5 on WordPress leading to topic deletion.	5.4	More Details
CVE-2022-40205	Insecure direct object references (IDOR) vulnerability in the wpForo Forum plugin <= 2.0.5 on WordPress allows attackers with subscriber or higher user roles to mark any forum post as solved/unsolved.	5.4	More Details
CVE-2022-43144	A cross-site scripting (XSS) vulnerability in Canteen Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44627	Cross-Site Request Forgery (CSRF) vulnerability in David Cole Simple SEO plugin <= 1.8.12 on WordPress allows attackers to create or delete sitemaps.	5.4	More Details
CVE-2022-20963	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, 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 code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker would need valid credentials to access the web-based management interface of an affected device.	5.4	More Details
CVE-2021-39473	Saibamen HotelManager v1.2 is vulnerable to Cross Site Scripting (XSS) due to improper sanitization of comment and contact fields.	5.4	More Details
CVE-2022-41435	OpenWRT LuCI version git-22.140.66206-02913be was discovered to contain a stored cross-site scripting (XSS) vulnerability in the component /system/sshkeys.js. This vulnerability allows attackers to execute arbitrary web scripts or HTML via crafted public key comments.	5.4	More Details
CVE-2022-20867	A vulnerability in web-based management interface of the of Cisco Email Security Appliance and Cisco Secure Email and Web Manager could allow an authenticated, remote attacker to conduct SQL injection attacks as root on an affected system. The attacker must have the credentials of a high-privileged user account. This vulnerability is due to improper validation of user-submitted parameters. An attacker could exploit this vulnerability by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain data or modify data that is stored in the underlying database of the affected system.	5.4	More Details
CVE-2022-38710	IBM Robotic Process Automation 21.0.1 and 21.0.2 could disclose sensitive version to an unauthorized control sphere information that could aid in further attacks against the system. IBM X-Force ID: 234292.	5.3	More Details
CVE-2022-20937	A vulnerability in a feature that monitors RADIUS requests on Cisco Identity Services Engine (ISE) Software could allow an unauthenticated, remote attacker to negatively affect the performance of an affected device. This vulnerability is due to insufficient management of system resources. An attacker could exploit this vulnerability by taking actions that cause Cisco ISE Software to receive specific RADIUS traffic. A successful and sustained exploit of this vulnerability could allow the attacker to cause reduced performance of the affected device, resulting in significant delays to RADIUS authentications. There are workarounds that address this vulnerability.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39069	There is a SQL injection vulnerability in ZTE ZAIP-AIE. Due to lack of input verification by the server, an attacker could trigger an attack by building malicious requests. Exploitation of this vulnerability could cause the leakage of the current table content.	5.3	More Details
CVE-2022-38381	An improper handling of malformed request vulnerability [CWE-228] exists in FortiADC 5.0 all versions, 6.0.0 all versions, 6.1.0 all versions, 6.2.0 through 6.2.3, and 7.0.0 through 7.0.2. This may allow a remote attacker without privileges to bypass some Web Application Firewall (WAF) protection such as the SQL Injection and XSS filters via a malformed HTTP request.	5.3	More Details
CVE-2022-27516	User login brute force protection functionality bypass	5.3	More Details
CVE-2022-41714	fastest-json-copy version 1.0.1 allows an external attacker to edit or add new properties to an object. This is possible because the application does not correctly validate the incoming JSON keys, thus allowing the '__proto__' property to be edited.	5.3	More Details
CVE-2022-42743	deep-parse-json version 1.0.2 allows an external attacker to edit or add new properties to an object. This is possible because the application does not correctly validate the incoming JSON keys, thus allowing the '__proto__' property to be edited.	5.3	More Details
CVE-2022-42473	A missing authentication for a critical function vulnerability in Fortinet FortiSOAR 6.4.0 - 6.4.4 and 7.0.0 - 7.0.3 and 7.2.0 allows an attacker to disclose information via logging into the database using a privileged account without a password.	5.3	More Details
CVE-2022-39378	Discourse is a platform for community discussion. Under certain conditions, a user badge may have been awarded based on a user's activity in a topic with restricted access. Before this vulnerability was disclosed, the topic title of the topic associated with the user badge may be viewed by any user. If there are sensitive information in the topic title, it will therefore have been exposed. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. There are currently no known workarounds available.	5.3	More Details
CVE-2022-41713	deep-object-diff version 1.1.0 allows an external attacker to edit or add new properties to an object. This is possible because the application does not properly validate incoming JSON keys, thus allowing the '__proto__' property to be edited.	5.3	More Details
CVE-2022-3489	The WP Hide WordPress plugin through 0.0.2 does not have authorisation and CSRF checks in place when updating the custom_wpadmin_slug settings, allowing unauthenticated attackers to update it with a crafted request	5.3	More Details
CVE-2022-30515	ZKTeco BioTime 8.5.4 is missing authentication on folders containing employee photos, allowing an attacker to view them through filename enumeration.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39262	GLPI stands for Gestionnaire Libre de Parc Informatique. GLPI is a Free Asset and IT Management Software package, GLPI administrator can define rich-text content to be displayed on login page. The displayed content is can contains malicious code that can be used to steal credentials. This issue has been patched, please upgrade to version 10.0.4.	5.2	More Details
CVE-2021-45446	A vulnerability in Hitachi Vantara Pentaho Business Analytics Server versions before 9.2.0.2 and 8.3.0.25 does not cascade the hidden property to the children of the Home folder. This directory listing provides an attacker with the complete index of all the resources located inside the directory.	5.0	More Details
CVE-2022-43564	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, a remote user who can create search macros and schedule search reports can cause a denial of service through the use of specially crafted search macros.	4.9	More Details
CVE-2021-37823	OpenCart 3.0.3.7 allows users to obtain database information or read server files through SQL injection in the background.	4.9	More Details
CVE-2022-39373	GLPI stands for Gestionnaire Libre de Parc Informatique. GLPI is a Free Asset and IT Management Software package that provides ITIL Service Desk features, licenses tracking and software auditing. Administrator may store malicious code in entity name. This issue has been patched, please upgrade to version 10.0.4.	4.9	More Details
CVE-2022-41212	Due to insufficient input validation, SAP NetWeaver Application Server ABAP and ABAP Platform allows an attacker with high level privileges to use a remote enabled function to read a file which is otherwise restricted. On successful exploitation an attacker can completely compromise the confidentiality of the application.	4.9	More Details
CVE-2022-41432	EyesOfNetwork Web Interface v5.3 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the component /module/report_event/index.php.	4.8	More Details
CVE-2022-36428	Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in Stage Rock Convert plugin <= 2.11.0 on WordPress.	4.8	More Details
CVE-2022-44628	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in JumpDEMAND Inc. 4ECPS Web Forms plugin <= 0.2.17 on WordPress.	4.8	More Details
CVE-2022-20969	A vulnerability in multiple management dashboard pages of Cisco Umbrella could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the Cisco Umbrella dashboard. This vulnerability is due to unsanitized user input. An attacker could exploit this vulnerability by submitting custom JavaScript to the web application and persuading a user of the interface to click a maliciously crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive browser-based information.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39352	OpenFGA is a high-performance authorization/permission engine inspired by Google Zanzibar. Versions prior to 0.2.5 are vulnerable to authorization bypass under certain conditions. You are affected by this vulnerability if you added a tuple with a wildcard (*) assigned to a tupleset relation (the right hand side of a 'from' statement). This issue has been patched in version v0.2.5. This update is not backward compatible with any authorization model that uses wildcard on a tupleset relation.	4.8	More Details
CVE-2022-3462	The Highlight Focus WordPress plugin through 1.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-41980	Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in Mantenimiento web plugin <= 0.13 on WordPress.	4.8	More Details
CVE-2022-41433	EyesOfNetwork Web Interface v5.3 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the component /module/admin_bp/add_application.php.	4.8	More Details
CVE-2022-30545	Auth. Reflected Cross-Site Scripting (XSS) vulnerability in 5 Anker Connect plugin <= 1.2.6 on WordPress.	4.8	More Details
CVE-2022-43372	Emlog Pro v1.7.1 was discovered to contain a reflected cross-site scripting (XSS) vulnerability at /admin/store.php.	4.8	More Details
CVE-2022-32776	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Advanced Ads GmbH Advanced Ads – Ad Manager & AdSense plugin <= 1.31.1 on WordPress.	4.8	More Details
CVE-2022-27894	The Foundry Blobster service was found to have a cross-site scripting (XSS) vulnerability that could have allowed an attacker with access to Foundry to launch attacks against other users. This vulnerability is resolved in Blobster 3.228.0.	4.8	More Details
CVE-2022-43046	Food Ordering Management System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the component /foms/place-order.php.	4.8	More Details
CVE-2022-44586	Auth. (admin+) Stored Cross-Site Scripting (XSS) in Ayoub Media AM-HiLi plugin <= 1.0 on WordPress.	4.8	More Details
CVE-2022-44576	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in AgentEasy Properties plugin <= 1.0.4 on WordPress.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20868	A vulnerability in the web-based management interface of Cisco Email Security Appliance, Cisco Secure Email and Web Manager and Cisco Secure Web Appliance could allow an authenticated, remote attacker to elevate privileges on an affected system. The attacker needs valid credentials to exploit this vulnerability. This vulnerability is due to the use of a hardcoded value to encrypt a token used for certain APIs calls . An attacker could exploit this vulnerability by authenticating to the device and sending a crafted HTTP request. A successful exploit could allow the attacker to impersonate another valid user and execute commands with the privileges of that user account.	4.7	More Details
CVE-2022-41215	SAP NetWeaver ABAP Server and ABAP Platform allows an unauthenticated attacker to redirect users to a malicious site due to insufficient URL validation. This could lead to the user being tricked to disclose personal information.	4.7	More Details
CVE-2022-20772	A vulnerability in Cisco Email Security Appliance (ESA) and Cisco Secure Email and Web Manager could allow an unauthenticated, remote attacker to conduct an HTTP response splitting attack. This vulnerability is due to the failure of the application or its environment to properly sanitize input values. An attacker could exploit this vulnerability by injecting malicious HTTP headers, controlling the response body, or splitting the response into multiple responses.	4.7	More Details
CVE-2022-26122	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version 6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad characters in base64.	4.7	More Details
CVE-2021-42205	ELAN Miniport touchpad Windows driver before 24.21.51.2, as used in PC hardware from multiple manufacturers, allows local users to cause a system crash by sending a certain IOCTL request, because that request is handled twice.	4.7	More Details
CVE-2022-39234	GLPI stands for Gestionnaire Libre de Parc Informatique. GLPI is a Free Asset and IT Management Software package that provides ITIL Service Desk features, licenses tracking and software auditing. Deleted/deactivated user could continue to use their account as long as its cookie is valid. This issue has been patched, please upgrade to version 10.0.4. There are currently no known workarounds.	4.7	More Details
CVE-2022-3868	A vulnerability classified as critical has been found in SourceCodester Sanitization Management System. Affected is an unknown function of the file /php-sms/classes/Master.php?f=save_quote. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-213012.	4.7	More Details
CVE-2022-20465	In dismiss and related functions of KeyguardHostViewController.java and related files, there is a possible lockscreen bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-218500036	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3721	Code Injection in GitHub repository froxlor/froxlor prior to 0.10.39.	4.6	More Details
CVE-2022-39375	GLPI stands for Gestionnaire Libre de Parc Informatique. GLPI is a Free Asset and IT Management Software package that provides ITIL Service Desk features, licenses tracking and software auditing. Users may be able to create a public RSS feed to inject malicious code in dashboards of other users. This issue has been patched, please upgrade to version 10.0.4. There are currently no known workarounds.	4.5	More Details
CVE-2022-39277	GLPI stands for Gestionnaire Libre de Parc Informatique. GLPI is a Free Asset and IT Management Software package that provides ITIL Service Desk features, licenses tracking and software auditing. External links are not properly sanitized and can therefore be used for a Cross-Site Scripting (XSS) attack. This issue has been patched, please upgrade to GLPI 10.0.4. There are currently no known workarounds.	4.5	More Details
CVE-2021-39077	IBM Security Guardium 10.5, 10.6, 11.0, 11.1, 11.2, 11.3, and 11.4 stores user credentials in plain clear text which can be read by a local privileged user. IBM X-Force ID: 215587.	4.4	More Details
CVE-2022-39949	An improper control of a resource through its lifetime vulnerability [CWE-664] in FortiEDR CollectorWindows 4.0.0 through 4.1, 5.0.0 through 5.0.3.751, 5.1.0 may allow a privileged user to terminate the FortiEDR processes with special tools and bypass the EDR protection.	4.4	More Details
CVE-2022-35279	"IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, and 22.0.1 could disclose sensitive version information to authenticated users which could be used in further attacks against the system. IBM X-Force ID: 230537."	4.3	More Details
CVE-2022-3810	A vulnerability was found in Axiomatic Bento4. It has been classified as problematic. This affects the function AP4_File::AP4_File of the file Mp42Hevc.cpp of the component mp42hevc. The manipulation leads to denial of service. 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-212667.	4.3	More Details
CVE-2022-39370	GLPI stands for Gestionnaire Libre de Parc Informatique. GLPI is a Free Asset and IT Management Software package that provides ITIL Service Desk features, licenses tracking and software auditing. Connected users may gain access to debug panel through the GLPI update script. This issue has been patched, please upgrade to 10.0.4. As a workaround, delete the `install/update.php` script.	4.3	More Details
CVE-2022-3826	A vulnerability was found in Huaxia ERP. It has been classified as problematic. This affects an unknown part of the file /depotHead/list of the component Retail Management. The manipulation of the argument search leads to information disclosure. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-212793 was assigned to this vulnerability.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35473	An information leakage vulnerability in the Bluetooth Low Energy advertisement scan response in Bluetooth Core Specifications 4.0 through 5.2, and extended scan response in Bluetooth Core Specifications 5.0 through 5.2, may be used to identify devices using Resolvable Private Addressing (RPA) by their response or non-response to specific scan requests from remote addresses. RPAs that have been associated with a specific remote device may also be used to identify a peer in the same manner by using its reaction to an active scan request. This has also been called an allowlist-based side channel.	4.3	More Details
CVE-2022-38380	An improper access control [CWE-284] vulnerability in FortiOS version 7.2.0 and versions 7.0.0 through 7.0.7 may allow a remote authenticated read-only user to modify the interface settings via the API.	4.3	More Details
CVE-2022-38137	Cross-Site Request Forgery (CSRF) vulnerability in Analytify plugin <= 4.2.2 on WordPress.	4.3	More Details
CVE-2022-40128	Cross-Site Request Forgery (CSRF) vulnerability in Advanced Order Export For WooCommerce plugin <= 3.3.2 on WordPress leading to export file download.	4.3	More Details
CVE-2022-3451	The Product Stock Manager WordPress plugin before 1.0.5 does not have authorisation and proper CSRF checks in multiple AJAX actions, allowing users with a role as low as subscriber to call them. One action in particular could allow to update arbitrary options	4.3	More Details
CVE-2022-2387	The Easy Digital Downloads WordPress plugin before 3.0 does not have CSRF check in place when deleting payment history, and does not ensure that the post to be deleted is actually a payment history. As a result, attackers could make a logged in admin delete arbitrary post via a CSRF attack	4.3	More Details
CVE-2022-3809	A vulnerability was found in Axiomatic Bento4 and classified as problematic. Affected by this issue is the function ParseCommandLine of the file Mp4Tag/Mp4Tag.cpp of the component mp4tag. The manipulation leads to denial of service. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-212666 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2022-25952	Cross-Site Request Forgery (CSRF) vulnerability in Keywordrush Content Egg plugin <= 5.4.0 on WordPress.	4.3	More Details
CVE-2022-27893	The Foundry Magritte plugin osisoft-pi-web-connector versions 0.15.0 - 0.43.0 was found to be logging in a manner that captured authentication requests. This vulnerability is resolved in osisoft-pi-web-connector version 0.44.0.	4.2	More Details
CVE-2022-30307	A key management error vulnerability [CWE-320] affecting the RSA SSH host key in FortiOS 7.2.0 and below, 7.0.6 and below, 6.4.9 and below may allow an unauthenticated attacker to perform a man in the middle attack.	3.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20962	A vulnerability in the Localdisk Management feature of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to make unauthorized changes to the file system of an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted HTTP request with absolute path sequences. A successful exploit could allow the attacker to upload malicious files to arbitrary locations within the file system. Using this method, it is possible to access the underlying operating system and execute commands with system privileges.	3.8	More Details
CVE-2022-35842	An exposure of sensitive information to an unauthorized actor vulnerabiltiy [CWE-200] in FortiOS SSL-VPN versions 7.2.0, versions 7.0.0 through 7.0.6 and versions 6.4.0 through 6.4.9 may allow a remote unauthenticated attacker to gain information about LDAP and SAML settings configured in FortiOS.	3.7	More Details
CVE-2022-3258	Incorrect Permission Assignment for Critical Resource vulnerability in HYPR Workforce Access on Windows allows Authentication Abuse.	3.7	More Details
CVE-2022-39372	GLPI stands for Gestionnaire Libre de Parc Informatique. GLPI is a Free Asset and IT Management Software package that provides ITIL Service Desk features, licenses tracking and software auditing. Authenticated users may store malicious code in their account information. This issue has been patched, please upgrade to version 10.0.4. There are currently no known workarounds.	3.5	More Details
CVE-2020-36608	A vulnerability, which was classified as problematic, has been found in Tribal Systems Zenario CMS. Affected by this issue is some unknown functionality of the file admin_organizer.js of the component Error Log Module. The manipulation leads to cross site scripting. The attack may be launched remotely. The name of the patch is dfd0afacb26c3682a847bea7b49ea440b63f3baa. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-212816.	3.5	More Details
CVE-2022-3844	A vulnerability, which was classified as problematic, was found in Webmin 2.001. Affected is an unknown function of the file xterm/index.cgi. The manipulation leads to basic cross site scripting. It is possible to launch the attack remotely. Upgrading to version 2.003 is able to address this issue. The patch is identified as d3d33af3c0c3fd3a889c84e287a038b7a457d811. It is recommended to upgrade the affected component. VDB-212862 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2022-39276	GLPI stands for Gestionnaire Libre de Parc Informatique. GLPI is a Free Asset and IT Management Software package that provides ITIL Service Desk features, licenses tracking and software auditing. Usage of RSS feeds or an external calendar in planning is subject to SSRF exploit. In case a remote script returns a redirect response, the redirect target URL is not checked against the URL allow list defined by administrator. This issue has been patched, please upgrade to 10.0.4. There are currently no known workarounds.	3.5	More Details
CVE-2022-38163	A Drag and Drop spoof vulnerability was discovered in F-Secure SAFE Browser for Android and iOS version 19.0 and below. Drag and drop operation by user on address bar could lead to a spoofing of the address bar.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42442	IBM Robotic Process Automation for Cloud Pak 21.0.1, 21.0.2, 21.0.3, 21.0.4, and 21.0.5 is vulnerable to exposure of the first tenant owner e-mail address to users with access to the container platform. IBM X-Force ID: 238214.	3.3	More Details
CVE-2022-20446	In AlwaysOnHotwordDetector of AlwaysOnHotwordDetector.java, there is a possible way to access the microphone from the background due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-229793943	3.3	More Details
CVE-2022-39379	Fluentd collects events from various data sources and writes them to files, RDBMS, NoSQL, IaaS, SaaS, Hadoop and so on. A remote code execution (RCE) vulnerability in non-default configurations of Fluentd allows unauthenticated attackers to execute arbitrary code via specially crafted JSON payloads. Fluentd setups are only affected if the environment variable `FLUENT_OJ_OPTION_MODE` is explicitly set to `object`. Please note: The option FLUENT_OJ_OPTION_MODE was introduced in Fluentd version 1.13.2. Earlier versions of Fluentd are not affected by this vulnerability. This issue was patched in version 1.15.3. As a workaround do not use `FLUENT_OJ_OPTION_MODE=object`.	3.1	More Details
CVE-2022-42494	Server Side Request Forgery (SSRF) vulnerability in All in One SEO Pro plugin <= 4.2.5.1 on WordPress.	3.0	More Details
CVE-2022-43562	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, Splunk Enterprise fails to properly validate and escape the Host header, which could let a remote authenticated user conduct various attacks against the system, including cross-site scripting and cache poisoning.	3.0	More Details
CVE-2022-44622	In JetBrains TeamCity version between 2021.2 and 2022.10 access permissions for secure token health items were excessive	2.7	More Details
CVE-2021-36906	Multiple Insecure Direct Object References (IDOR) vulnerabilities in ExpressTech Quiz And Survey Master plugin <= 7.3.6 on WordPress.	2.7	More Details
CVE-2022-3675	Fedora CoreOS supports setting a GRUB bootloader password using a Butane config. When this feature is enabled, GRUB requires a password to access the GRUB command-line, modify kernel command-line arguments, or boot non-default OSTree deployments. Recent Fedora CoreOS releases have a misconfiguration which allows booting non-default OSTree deployments without entering a password. This allows someone with access to the GRUB menu to boot into an older version of Fedora CoreOS, reverting any security fixes that have recently been applied to the machine. A password is still required to modify kernel command-line arguments and to access the GRUB command line.	2.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39376	GLPI stands for Gestionnaire Libre de Parc Informatique. GLPI is a Free Asset and IT Management Software package that provides ITIL Service Desk features, licenses tracking and software auditing. Users may be able to inject custom fields values in `mailto` links. This issue has been patched, please upgrade to version 10.0.4. There are currently no known workarounds.	2.6	More Details
CVE-2022-3845	A vulnerability has been found in phpipam and classified as problematic. Affected by this vulnerability is an unknown functionality of the file app/admin/import-export/import-load-data.php of the component Import Preview Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. Upgrading to version 1.5.0 is able to address this issue. The name of the patch is 22c797c3583001211fe7d31bccd3f1d4aeeb3bbc. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-212863.	2.4	More Details
CVE-2022-44646	In JetBrains TeamCity version before 2022.10, no audit items were added upon editing a user's settings	2.2	More Details
CVE-2022-33878	An exposure of sensitive information to an unauthorized actor vulnerabiltiy [CWE-200] in FortiClient for Mac versions 7.0.0 through 7.0.5 may allow a local authenticated attacker to obtain the SSL-VPN password in cleartext via running a logstream for the FortiTray process in the terminal.	2.2	More Details
CVE-2021-34686	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn. Further investigation showed that it was not a vulnerability. Notes: none.	N/A	More Details
CVE-2021-41574	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn. Further investigation showed that it was not a vulnerability. Notes: none.	N/A	More Details
CVE-2022-24945	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-2021-41575	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn. Further investigation showed that it was not a vulnerability. Notes: none.	N/A	More Details
CVE-2021-41576	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn. Further investigation showed that it was not a vulnerability. Notes: none.	N/A	More Details
CVE-2022-20463	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