SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 07 September 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-2022-21941	All versions of iSTAR Ultra prior to version 6.8.9.CU01 are vulnerable to a command injection that could allow an unauthenticated user root access to the system.	10.0	More Details
CVE-2022-36067	vm2 is a sandbox that can run untrusted code with whitelisted Node's built-in modules. In versions prior to version 3.9.11, a threat actor can bypass the sandbox protections to gain remote code execution rights on the host running the sandbox. This vulnerability was patched in the release of version 3.9.11 of vm2. There are no known workarounds.	10.0	More Details
CVE-2022-36130	HashiCorp Boundary up to 0.10.1 did not properly perform data integrity checks to ensure the resources were associated with the correct scopes, allowing potential privilege escalation for authorized users of another scope. Fixed in Boundary 0.10.2.	9.9	More Details
CVE-2022-37021	Apache Geode versions up to 1.12.5, 1.13.4 and 1.14.0 are vulnerable to a deserialization of untrusted data flaw when using JMX over RMI on Java 8. Any user still on Java 8 who wishes to protect against deserialization attacks involving JMX or RMI should upgrade to Apache Geode 1.15 and Java 11. If upgrading to Java 11 is not possible, then upgrade to Apache Geode 1.15 and specify "--J=-Dgeode.enableGlobalSerialFilter=true" when starting any Locators or Servers. Follow the documentation for details on specifying any user classes that may be serialized/deserialized with the "serializable-object-filter" configuration option. Using a global serial filter will impact performance.	9.8	More Details
CVE-2022-37842	In TOTOLINK A860R V4.1.2cu.5182_B20201027, the parameters in infostat.cgi are not filtered, causing a buffer overflow vulnerability.	9.8	More Details
CVE-2021-27693	Server-side Request Forgery (SSRF) vulnerability in PublicCMS before 4.0.202011.b via /publiccms/admin/ueditor when the action is catchimage.	9.8	More Details
CVE-2022-36640	influxData influxDB before v1.8.10 contains no authentication mechanism or controls, allowing unauthenticated attackers to execute arbitrary commands. NOTE: the CVE ID assignment is disputed because the vendor's documentation states "If InfluxDB is being deployed on a publicly accessible endpoint, we strongly recommend authentication be enabled. Otherwise the data will be publicly available to any unauthenticated user. The default settings do NOT enable authentication and authorization.	9.8	More Details
CVE-2022-36642	A local file disclosure vulnerability in /appConfig/userDB.json of Telos Alliance Omnia MPX Node through 1.0.0-1.4.9 allows attackers to access users credentials which makes him able to gain initial access to the control panel with high privilege because the cleartext storage of sensitive information which can be unlatched by exploiting the LFD vulnerability.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31814	pfSense pfBlockerNG through 2.1.4_26 allows remote attackers to execute arbitrary OS commands as root via shell metacharacters in the HTTP Host header. NOTE: 3.x is unaffected.	9.8	More Details
CVE-2022-34747	A format string vulnerability in Zyxel NAS326 firmware versions prior to V5.21(AAZF.12)C0 could allow an attacker to achieve unauthorized remote code execution via a crafted UDP packet.	9.8	More Details
CVE-2022-2714	Improper Handling of Length Parameter Inconsistency in GitHub repository francoisjacquet/rosariosis prior to 10.0.	9.8	More Details
CVE-2022-36584	In Tenda G3 US_G3V3.0br_V15.11.0.6(7663)_EN_TDE, the getsinglepppuser function has a buffer overflow caused by sscanf.	9.8	More Details
CVE-2022-37839	TOTOLINK A860R V4.1.2cu.5182_B20201027 is vulnerable to Buffer Overflow via Cstecgi.cgi.	9.8	More Details
CVE-2022-37840	In TOTOLINK A860R V4.1.2cu.5182_B20201027, the main function in downloadfile.cgi has a buffer overflow vulnerability.	9.8	More Details
CVE-2022-37843	In TOTOLINK A860R V4.1.2cu.5182_B20201027 in cstecgi.cgi, the acquired parameters are directly put into the system for execution without filtering, resulting in a command injection vulnerability.	9.8	More Details
CVE-2022-22096	Memory corruption in Bluetooth HOST due to stack-based buffer overflow when when extracting data using command length parameter in Snapdragon Connectivity, Snapdragon Mobile	9.8	More Details
CVE-2022-40109	TOTOLINK A3002R TOTOLINK-A3002R-He-V1.1.1-B20200824.0128 is vulnerable to Insecure Permissions via binary /bin/boa.	9.8	More Details
CVE-2022-40111	In TOTOLINK A3002R TOTOLINK-A3002R-He-V1.1.1-B20200824.0128 in the shadow.sample file, root is hardcoded in the firmware.	9.8	More Details
CVE-2022-26447	In BT firmware, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06784478; Issue ID: ALPS06784478.	9.8	More Details
CVE-2022-31860	An issue was discovered in OpenRemote through 1.0.4 allows attackers to execute arbitrary code via a crafted Groovy rule.	9.8	More Details
CVE-2020-21516	There is an arbitrary file upload vulnerability in FeehiCMS 2.0.8 at the head image upload, that allows attackers to execute relevant PHP code.	9.8	More Details
CVE-2022-31789	An integer overflow in WatchGuard Firebox and XTM appliances allows an unauthenticated remote attacker to trigger a buffer overflow and potentially execute arbitrary code by sending a malicious request to exposed management ports. This is fixed in Fireware OS 12.8.1, 12.5.10, and 12.1.4.	9.8	More Details
CVE-2022-36663	Gluu Oxauth before v4.4.1 allows attackers to execute blind SSRF (Server-Side Request Forgery) attacks via a crafted request_uri parameter.	9.8	More Details
CVE-2022-1368	The Cognex 3D-A1000 Dimensioning System in firmware version 1.0.3 (3354) and prior is vulnerable to CWE-306: Missing Authentication for Critical Function, which allows unauthorized users to change the operator account password via webserver commands by monitoring web socket communications from an unauthenticated session. This could allow an attacker to escalate privileges to match those of the compromised account.	9.8	More Details
CVE-2020-22669	Modsecurity owasp-modsecurity-crs 3.2.0 (Paranoia level at PL1) has a SQL injection bypass vulnerability. Attackers can use the comment characters and variable assignments in the SQL syntax to bypass Modsecurity WAF protection and implement SQL injection attacks on Web applications.	9.8	More Details
CVE-2022-38054	In Apache Airflow versions 2.2.4 through 2.3.3, the `database` webserver session backend was susceptible to session fixation.	9.8	More Details
CVE-2020-35527	In SQLite 3.31.1, there is an out of bounds access problem through ALTER TABLE for views that have a nested FROM clause.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36566	Rengine v1.3.0 was discovered to contain a command injection vulnerability via the scan engine function.	9.8	More Details
CVE-2022-36201	Doctor’s Appointment System v1.0 is vulnerable to Blind SQLi via settings.php.	9.8	More Details
CVE-2022-36202	Doctor's Appointment System1.0 is vulnerable to Incorrect Access Control via edoc/patient/settings.php. The settings.php is affected by Broken Access Control (IDOR) via id= parameter.	9.8	More Details
CVE-2022-37125	D-link DIR-816 A2_v1.10CNB04.img is vulnerable to Command injection via /goform/NTPSyncWithHost.	9.8	More Details
CVE-2022-37130	In D-Link DIR-816 A2_v1.10CNB04, DIR-878 DIR_878_FW1.30B08.img a command injection vulnerability occurs in /goform/Diagnosis, after the condition is met, setnum will be spliced into v10 by snprintf, and the system will be executed, resulting in a command injection vulnerability	9.8	More Details
CVE-2022-36672	Novel-Plus v3.6.2 was discovered to contain a hard-coded JWT key located in the project config file. This vulnerability allows attackers to create a custom user session.	9.8	More Details
CVE-2022-30318	Honeywell ControlEdge through R151.1 uses Hard-coded Credentials. According to FSCT-2022-0056, there is a Honeywell ControlEdge hardcoded credentials issue. The affected components are characterized as: SSH. The potential impact is: Remote code execution, manipulate configuration, denial of service. The Honeywell ControlEdge PLC and RTU product line exposes an SSH service on port 22/TCP. Login as root to this service is permitted and credentials for the root user are hardcoded without automatically changing them upon first commissioning. The credentials for the SSH service are hardcoded in the firmware. The credentials grant an attacker access to a root shell on the PLC/RTU, allowing for remote code execution, configuration manipulation and denial of service.	9.8	More Details
CVE-2022-34372	Dell PowerProtect Cyber Recovery versions before 19.11.0.2 contain an authentication bypass vulnerability. A remote unauthenticated attacker may potentially access and interact with the docker registry API leading to an authentication bypass. The attacker may potentially alter the docker images leading to a loss of integrity and confidentiality	9.8	More Details
CVE-2022-37128	In D-Link DIR-816 A2_v1.10CNB04.img the network can be initialized without authentication via /goform/wizard_end.	9.8	More Details
CVE-2022-2466	It was found that Quarkus 2.10.x does not terminate HTTP requests header context which may lead to unpredictable behavior.	9.8	More Details
CVE-2022-36601	The Eclipse TCF debug interface in JasMiner-X4-Server-20220621-090907 and below is open on port 1534. This issue allows unauthenticated attackers to gain root privileges on the affected device and access sensitive data or execute arbitrary commands.	9.8	More Details
CVE-2022-36759	Online Food Ordering System v1.0 was discovered to contain a SQL injection vulnerability via the component /dishes.php?res_id=.	9.8	More Details
CVE-2022-36594	Mapper v4.0.0 to v4.2.0 was discovered to contain a SQL injection vulnerability via the ids parameter at the selectByIds function.	9.8	More Details
CVE-2022-36609	Clinic's Patient Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /pms/update_patient.php.	9.8	More Details
CVE-2022-25371	Apache OFBiz uses the Birt project plugin (https://eclipse.github.io/birt-website/) to create data visualizations and reports. By leveraging a bug in Birt (https://bugs.eclipse.org/bugs/show_bug.cgi?id=538142) it is possible to perform a remote code execution (RCE) attack in Apache OFBiz, release 18.12.05 and earlier.	9.8	More Details
CVE-2022-29063	The Solr plugin of Apache OFBiz is configured by default to automatically make a RMI request on localhost, port 1099. In version 18.12.05 and earlier, by hosting a malicious RMI server on localhost, an attacker may exploit this behavior, at server start-up or on a server restart, in order to run arbitrary code. Upgrade to at least 18.12.06 or apply patches at https://issues.apache.org/jira/browse/OFBIZ-12646.	9.8	More Details
CVE-2022-2485	Any attempt (good or bad) to log into AutomationDirect Stride Field I/O with a web browser may result in the device responding with its password in the communication packets.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34379	Dell EMC CloudLink 7.1.2 and all prior versions contain an Authentication Bypass Vulnerability. A remote attacker, with the knowledge of the active directory usernames, could potentially exploit this vulnerability to gain unauthorized access to the system.	9.4	More Details
CVE-2021-35122	Non-secure region can try modifying RG permissions of IO space xPUs due to improper input validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	9.3	More Details
CVE-2022-34380	Dell CloudLink 7.1.3 and all earlier versions contain an Authentication Bypass Using an Alternate Path or Channel Vulnerability. A high privileged local attacker may potentially exploit this vulnerability leading to authentication bypass and access the CloudLink system console. This is critical severity vulnerability as it allows attacker to take control of the system.	9.3	More Details
CVE-2022-30317	Honeywell Experion LX through 2022-05-06 has Missing Authentication for a Critical Function. According to FSCT-2022-0055, there is a Honeywell Experion LX Control Data Access (CDA) EpicMo protocol with unauthenticated functionality issue. The affected components are characterized as: Honeywell Control Data Access (CDA) EpicMo (55565/TCP). The potential impact is: Firmware manipulation, Denial of service. The Honeywell Experion LX Distributed Control System (DCS) utilizes the Control Data Access (CDA) EpicMo protocol (55565/TCP) for device diagnostics and maintenance purposes. This protocol does not have any authentication features, allowing any attacker capable of communicating with the ports in question to invoke (a subset of) desired functionality. There is no authentication functionality on the protocol in question. An attacker capable of invoking the protocols' functionalities could issue firmware download commands potentially allowing for firmware manipulation and reboot devices causing denial of service.	9.1	More Details
CVE-2022-1525	The Cognex 3D-A1000 Dimensioning System in firmware version 1.0.3 (3354) and prior is vulnerable to CWE-602: Client-Side Enforcement of Server-Side Security, which could allow attackers to bypass web access controls by inspecting and modifying the source code of password protected web elements.	9.1	More Details
CVE-2022-36045	NodeBB Forum Software is powered by Node.js and supports either Redis, MongoDB, or a PostgreSQL database. It utilizes web sockets for instant interactions and real-time notifications. `utils.generateUUID`, a helper function available in essentially all versions of NodeBB (as far back as v1.0.1 and potentially earlier) used a cryptographically insecure Pseudo-random number generator (`Math.random()`), which meant that a specially crafted script combined with multiple invocations of the password reset functionality could enable an attacker to correctly calculate the reset code for an account they do not have access to. This vulnerability impacts all installations of NodeBB. The vulnerability allows for an attacker to take over any account without the involvement of the victim, and as such, the remediation should be applied immediately (either via NodeBB upgrade or cherry-pick of the specific changeset. The vulnerability has been patched in version 2.x and 1.19.x. There is no known workaround, but the patch sets listed above will fully patch the vulnerability.	9.0	More Details
CVE-2022-34882	Information Exposure Through an Error Message vulnerability in Hitachi RAID Manager Storage Replication Adapter allows remote authenticated users to gain sensitive information. This issue affects: Hitachi RAID Manager Storage Replication Adapter 02.01.04 versions prior to 02.03.02 on Windows; 02.05.00 versions prior to 02.05.01 on Windows and Docker.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-39824	Server-side JavaScript injection in Appsmith through 1.7.14 allows remote attackers to execute arbitrary JavaScript code from the server via the currentItem property of the list widget, e.g., to perform DoS attacks or achieve an information leak.	8.9	More Details
CVE-2022-1902	A flaw was found in the Red Hat Advanced Cluster Security for Kubernetes. Notifier secrets were not properly sanitized in the GraphQL API. This flaw allows authenticated ACS users to retrieve Notifiers from the GraphQL API, revealing secrets that can escalate their privileges.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23679	AOS-CX lacks Anti-CSRF protections in place for state-changing operations. This can potentially be exploited by an attacker to execute commands in the context of another user in ArubaOS-CX Switches version(s): AOS-CX 10.10.xxxx: 10.10.0002 and below, AOS-CX 10.09.xxxx: 10.09.1020 and below, AOS-CX 10.08.xxxx: 10.08.1060 and below, AOS-CX 10.06.xxxx: 10.06.0200 and below. Aruba has released upgrades for ArubaOS-CX Switch Devices that address this security vulnerability.	8.8	More Details
CVE-2022-2434	The String Locator plugin for WordPress is vulnerable to deserialization of untrusted input via the 'string-locator-path' parameter in versions up to, and including 2.5.0. This makes it possible for unauthenticated users to call files using a PHAR wrapper, granted they can trick a site administrator into performing an action such as clicking on a link, that will deserialize and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.	8.8	More Details
CVE-2022-2433	The WordPress Infinite Scroll – Ajax Load More plugin for WordPress is vulnerable to deserialization of untrusted input via the 'alm_repeaters_export' parameter in versions up to, and including 5.5.3. This makes it possible for unauthenticated users to call files using a PHAR wrapper, granted they can trick a site administrator into performing an action such as clicking on a link, that will deserialize and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.	8.8	More Details
CVE-2022-2432	The Ecwid Ecommerce Shopping Cart plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 6.10.23. This is due to missing or incorrect nonce validation on the ecwid_update_plugin_params function. This makes it possible for unauthenticated attackers to update plugin options granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2022-39047	Freeciv before 2.6.7 and before 3.0.3 is prone to a buffer overflow vulnerability in the Modpack Installer utility's handling of the modpack URL.	8.8	More Details
CVE-2022-2233	The Banner Cycler plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including 1.4. This is due to missing nonce protection on the pabc_admin_slides_postback() function found in the ~/admin/admin.php file. This makes it possible for unauthenticated attackers to inject malicious web scripts into the page, granted they can trick a site’s administrator into performing an action such as clicking on a link	8.8	More Details
CVE-2022-23684	A vulnerability in the web-based management interface of AOS-CX could allow a remote authenticated user with read-only privileges to escalate their permissions to those of an administrative user. Successful exploitation of this vulnerability allows an attacker to escalate privileges beyond their authorized level in ArubaOS-CX Switches version(s): AOS-CX 10.09.xxxx: 10.09.1020 and below, AOS-CX 10.08.xxxx: 10.08.1060 and below, AOS-CX 10.06.xxxx: 10.06.0200 and below. Aruba has released upgrades for ArubaOS-CX Switch Devices that address this security vulnerability.	8.8	More Details
CVE-2022-23680	AOS-CX lacks Anti-CSRF protections in place for state-changing operations. This can potentially be exploited by an attacker to execute commands in the context of another user in ArubaOS-CX Switches version(s): AOS-CX 10.10.xxxx: 10.10.0002 and below, AOS-CX 10.09.xxxx: 10.09.1020 and below, AOS-CX 10.08.xxxx: 10.08.1060 and below, AOS-CX 10.06.xxxx: 10.06.0200 and below. Aruba has released upgrades for ArubaOS-CX Switch Devices that address this security vulnerability.	8.8	More Details
CVE-2022-31020	Indy Node is the server portion of a distributed ledger purpose-built for decentralized identity. In versions 1.12.4 and prior, the `pool-upgrade` request handler in Indy-Node allows an improperly authenticated attacker to remotely execute code on nodes within the network. The `pool-upgrade` request handler in Indy-Node 1.12.5 has been updated to properly authenticate pool-upgrade transactions before any processing is performed by the request handler. The transactions are further sanitized to prevent remote code execution. As a workaround, endorsers should not create DIDs for untrusted users. A vulnerable ledger should configure `auth_rules` to prevent new DIDs from being written to the ledger until the network can be upgraded.	8.8	More Details
CVE-2022-1552	A flaw was found in PostgreSQL. There is an issue with incomplete efforts to operate safely when a privileged user is maintaining another user's objects. The Autovacuum, REINDEX, CREATE INDEX, REFRESH MATERIALIZED VIEW, CLUSTER, and pg_amcheck commands activated relevant protections too late or not at all during the process. This flaw allows an attacker with permission to create non-temporary objects in at least one schema to execute arbitrary SQL functions under a superuser identity.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30331	The User-Defined Functions (UDF) feature in TigerGraph 3.6.0 allows installation of a query (in the GSQL query language) without proper validation. Consequently, an attacker can execute arbitrary C++ code. NOTE: the vendor's position is "GSQL was behaving as expected."	8.8	More Details
CVE-2022-2830	Deserialization of Untrusted Data vulnerability in the message processing component of Bitdefender GravityZone Console allows an attacker to pass unsafe commands to the environment. This issue affects: Bitdefender GravityZone Console On-Premise versions prior to 6.29.2-1. Bitdefender GravityZone Cloud Console versions prior to 6.27.2-2.	8.8	More Details
CVE-2022-38369	Apache IoTDB version 0.13.0 is vulnerable by session id attack. Users should upgrade to version 0.13.1 which addresses this issue.	8.8	More Details
CVE-2022-36076	NodeBB Forum Software is powered by Node.js and supports either Redis, MongoDB, or a PostgreSQL database. Due to an unnecessarily strict conditional in the code handling the first step of the SSO process, the pre-existing logic that added (and later checked) a nonce was inadvertently rendered opt-in instead of opt-out. This re-exposed a vulnerability in that a specially crafted Man-in-the-Middle (MITM) attack could theoretically take over another user account during the single sign-on process. The issue has been fully patched in version 1.17.2.	8.8	More Details
CVE-2022-36569	Tenda AC9 V15.03.05.19 was discovered to contain a stack overflow via the deviceList parameter at /goform/setMacFilterCfg.	8.8	More Details
CVE-2022-37184	The application manage_website.php on Garage Management System 1.0 is vulnerable to Shell File Upload. The already authenticated malicious user, can upload a dangerous RCE or LCE exploit file.	8.8	More Details
CVE-2022-36568	Tenda AC9 V15.03.05.19 was discovered to contain a stack overflow via the list parameter at /goform/setPptpUserList.	8.8	More Details
CVE-2022-2436	The Download Manager plugin for WordPress is vulnerable to deserialization of untrusted input via the 'file[package_dir]' parameter in versions up to, and including 3.2.49. This makes it possible for authenticated attackers with contributor privileges and above to call files using a PHAR wrapper that will deserialize the data and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.	8.8	More Details
CVE-2022-36078	Binary provides encoding/decoding in Borsh and other formats. The vulnerability is a memory allocation vulnerability that can be exploited to allocate slices in memory with (arbitrary) excessive size value, which can either exhaust available memory or crash the whole program. When using `github.com/gagliardetto/binary` to parse unchecked (or wrong type of) data from untrusted sources of input (e.g. the blockchain) into slices, it's possible to allocate memory with excessive size. When `dec.Decode(&val)` method is used to parse data into a structure that is or contains slices of values, the length of the slice was previously read directly from the data itself without any checks on the size of it, and then a slice was allocated. This could lead to an overflow and an allocation of memory with excessive size value. Users should upgrade to `v0.7.1` or higher. A workaround is not to rely on the `dec.Decode(&val)` function to parse the data, but to use a custom `UnmarshalWithDecoder()` method that reads and checks the length of any slice.	8.8	More Details
CVE-2022-2518	The Stockists Manager for Woocommerce plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.0.2.1. This is due to missing nonce validation on the stockist_settings_main() function. This makes it possible for unauthenticated attackers to modify the plugin's settings and inject malicious web scripts 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-2022-2540	The Link Optimizer Lite plugin for WordPress is vulnerable to Cross-Site Request Forgery to Cross-Site Scripting in versions up to, and including 1.4.5. This is due to missing nonce validation on the admin_page function found in the ~/admin.php file. This makes it possible for unauthenticated attackers to modify the plugin's settings and inject malicious web scripts 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 Number	Description	Base Score	Reference
CVE-2022-37022	Apache Geode versions up to 1.12.2 and 1.13.2 are vulnerable to a deserialization of untrusted data flaw when using JMX over RMI on Java 11. Any user wishing to protect against deserialization attacks involving JMX or RMI should upgrade to Apache Geode 1.15. Use of 1.15 on Java 11 will automatically protect JMX over RMI against deserialization attacks. This should have no impact on performance since it only affects JMX/RMI which Gfsh uses to communicate with the JMX Manager which is hosted on a Locator.	8.8	More Details
CVE-2022-37435	Apache ShenYu Admin has insecure permissions, which may allow low-privilege administrators to modify high-privilege administrator's passwords. This issue affects Apache ShenYu 2.4.2 and 2.4.3.	8.8	More Details
CVE-2022-36602	InnoSilicon A10 a10_20200924_120556 was discovered to contain a remote code execution (RCE) vulnerability in the setPlatformAPI function.	8.8	More Details
CVE-2022-36603	InnoSilicon T3T+ t2t+_soc_20190911_151433.swu was discovered to contain a remote code execution (RCE) vulnerability in the checkUrl function.	8.8	More Details
CVE-2022-39170	libdwarf 0.4.1 has a double free in _dwarf_exec_frame_instr in dwarf_frame.c.	8.8	More Details
CVE-2022-39176	BlueZ before 5.59 allows physically proximate attackers to obtain sensitive information because profiles/audio/avrcp.c does not validate params_len.	8.8	More Details
CVE-2022-39177	BlueZ before 5.59 allows physically proximate attackers to cause a denial of service because malformed and invalid capabilities can be processed in profiles/audio/avdtp.c.	8.8	More Details
CVE-2022-36636	Garage Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /print.php.	8.8	More Details
CVE-2022-37129	D-Link DIR-816 A2_v1.10CNB04.img is vulnerable to Command Injection via /goform/SystemCommand. After the user passes in the command parameter, it will be spliced into byte_4836B0 by snprintf, and finally doSystem(&byte_4836B0); will be executed, resulting in a command injection.	8.8	More Details
CVE-2022-2541	The uContext for Amazon plugin for WordPress is vulnerable to Cross-Site Request Forgery to Cross-Site Scripting in versions up to, and including 3.9.1. This is due to missing nonce validation in the ~/app/sites/ajax/actions/keyword_save.php file that is called via the doAjax() function. This makes it possible for unauthenticated attackers to modify the plugin's settings and inject malicious web scripts 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-2022-1271	An arbitrary file write vulnerability was found in GNU gzip's zgrep utility. When zgrep is applied on the attacker's chosen file name (for example, a crafted file name), this can overwrite an attacker's content to an arbitrary attacker-selected file. This flaw occurs due to insufficient validation when processing filenames with two or more newlines where selected content and the target file names are embedded in crafted multi-line file names. This flaw allows a remote, low privileged attacker to force zgrep to write arbitrary files on the system.	8.8	More Details
CVE-2022-2542	The uContext for Clickbank plugin for WordPress is vulnerable to Cross-Site Request Forgery to Cross-Site Scripting in versions up to, and including 3.9.1. This is due to missing nonce validation in the ~/app/sites/ajax/actions/keyword_save.php file that is called via the doAjax() function. This makes it possible for unauthenticated attackers to modify the plugin's settings and inject malicious web scripts 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-2022-37123	D-link DIR-816 A2_v1.10CNB04.img is vulnerable to Command injection via /goform/form2userconfig.cgi.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36038	CircuitVerse is an open-source platform which allows users to construct digital logic circuits online. A remote code execution (RCE) vulnerability in CircuitVerse allows authenticated attackers to execute arbitrary code via specially crafted JSON payloads. This issue may lead to Remote Code Execution (RCE). A patch is available in commit number 7b3023a99499a7675f10f2c1d9effdf10c35fb6e. There are currently no known workarounds.	8.8	More Details
CVE-2022-36051	ZITADEL combines the ease of Auth0 and the versatility of Keycloak.**Actions**, introduced in ZITADEL **1.42.0** on the API and **1.56.0** for Console, is a feature, where users with role.`ORG_OWNER` are able to create Javascript Code, which is invoked by the system at certain points during the login. **Actions**, for example, allow creating authorizations (user grants) on newly created users programmatically. Due to a missing authorization check, **Actions** were able to grant authorizations for projects that belong to other organizations inside the same Instance. Granting authorizations via API and Console is not affected by this vulnerability. There is currently no known workaround, users should update.	8.7	More Details
CVE-2022-2132	A permissive list of allowed inputs flaw was found in DPDK. This issue allows a remote attacker to cause a denial of service triggered by sending a crafted Vhost header to DPDK.	8.6	More Details
CVE-2022-39838	Systematic FIX Adapter (ALFAFX) 2.4.0.25 13/09/2017 allows remote file inclusion via a UNC share pathname, and also allows absolute path traversal to local pathnames.	8.6	More Details
CVE-2022-22106	Memory corruption in multimedia due to improper length check while copying the data in Snapdragon Auto	8.4	More Details
CVE-2022-22059	Memory corruption due to out of bound read while parsing a video file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	8.4	More Details
CVE-2022-25680	Memory corruption in multimedia due to buffer overflow while processing count variable from client in Snapdragon Auto	8.4	More Details
CVE-2022-22099	Memory corruption in multimedia due to improper validation of array index in Snapdragon Auto	8.4	More Details
CVE-2022-22080	Improper validation of backend id in PCM routing process can lead to memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	8.4	More Details
CVE-2022-22100	Memory corruption in multimedia due to improper check on received export descriptors in Snapdragon Auto	8.4	More Details
CVE-2022-22098	Memory corruption in multimedia driver due to untrusted pointer dereference while reading data from socket in Snapdragon Auto	8.4	More Details
CVE-2021-35132	Out of bound write in DSP service due to improper bound check for response buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	8.4	More Details
CVE-2022-22104	Memory corruption in multimedia due to improper check on the messages received. in Snapdragon Auto	8.4	More Details
CVE-2021-35134	Due to insufficient validation of ELF headers, an Incorrect Calculation of Buffer Size can occur in Boot leading to memory corruption in Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22102	Memory corruption in multimedia due to incorrect type conversion while adding data in Snapdragon Auto	8.4	More Details
CVE-2022-22097	Memory corruption in graphic driver due to use after free while calling multiple threads application to driver. in Snapdragon Consumer IOT	8.4	More Details
CVE-2022-36071	SFTPGo is configurable SFTP server with optional HTTP/S, FTP/S and WebDAV support. SFTPGo WebAdmin and WebClient support login using TOTP (Time-based One Time Passwords) as a secondary authentication factor. Because TOTPs are often configured on mobile devices that can be lost, stolen or damaged, SFTPGo also supports recovery codes. These are a set of one time use codes that can be used instead of the TOTP. In SFTPGo versions from version 2.2.0 to 2.3.3 recovery codes can be generated before enabling two-factor authentication. An attacker who knows the user's password could potentially generate some recovery codes and then bypass two-factor authentication after it is enabled on the account at a later time. This issue has been fixed in version 2.3.4. Recovery codes can now only be generated after enabling two-factor authentication and are deleted after disabling it.	8.3	More Details
CVE-2022-31176	Grafana Image Renderer is a Grafana backend plugin that handles rendering of panels & dashboards to PNGs using a headless browser (Chromium/Chrome). An internal security review identified an unauthorized file disclosure vulnerability. It is possible for a malicious user to retrieve unauthorized files under some network conditions or via a fake datasource (if user has admin permissions in Grafana). All Grafana installations should be upgraded to version 3.6.1 as soon as possible. As a workaround it is possible to [disable HTTP remote rendering](https://grafana.com/docs/grafana/latest/setup-grafana/configure-grafana/#plugingrafana-image-renderer).	8.3	More Details
CVE-2022-2044	MOXA NPort 5110: Firmware Versions 2.10 is vulnerable to an out-of-bounds write that may allow an attacker to overwrite values in memory, causing a denial-of-service condition or potentially bricking the device.	8.2	More Details
CVE-2022-22062	An out-of-bounds read can occur while parsing a server certificate due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	8.2	More Details
CVE-2022-34369	Dell PowerScale OneFS, versions 9.0.0 up to and including 9.1.0.20, 9.2.1.13, 9.3.0.6, and 9.4.0.3 , contain an insertion of sensitive information in log files vulnerability. A remote unprivileged attacker could potentially exploit this vulnerability, leading to exposure of this sensitive data.	8.1	More Details
CVE-2022-34383	Dell Edge Gateway 5200 (EGW) versions before 1.03.10 contain an operating system command injection vulnerability. A local malicious user may potentially exploit this vulnerability by using an SMI to bypass PMC mitigation and gain arbitrary code execution during SMM.	8.1	More Details
CVE-2022-36773	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.2.1 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: 233571.	8.1	More Details
CVE-2022-2431	The Download Manager plugin for WordPress is vulnerable to arbitrary file deletion in versions up to, and including 3.2.50. This is due to insufficient file type and path validation on the deleteFiles() function found in the ~/Admin/Menu/Packages.php file that triggers upon download post deletion. This makes it possible for contributor level users and above to supply an arbitrary file path via the 'file[files]' parameter when creating a download post and once the user deletes the post the supplied arbitrary file will be deleted. This can be used by attackers to delete the /wp-config.php file which will reset the installation and make it possible for an attacker to achieve remote code execution on the server.	8.1	More Details
CVE-2022-3008	The tinygltf library uses the C library function wordexp() to perform file path expansion on untrusted paths that are provided from the input file. This function allows for command injection by using backticks. An attacker could craft an untrusted path input that would result in a path expansion. We recommend upgrading to 2.6.0 or past commit 52ff00a38447f06a17eab1caa2cf0730a119c751	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23451	An authorization flaw was found in openstack-barbican. The default policy rules for the secret metadata API allowed any authenticated user to add, modify, or delete metadata from any secret regardless of ownership. This flaw allows an attacker on the network to modify or delete protected data, causing a denial of service by consuming protected resources.	8.1	More Details
CVE-2022-34371	Dell PowerScale OneFS, versions 9.0.0 up to and including 9.1.0.19, 9.2.1.12, 9.3.0.6, and 9.4.0.3, contain an unprotected transport of credentials vulnerability. A malicious unprivileged network attacker could potentially exploit this vulnerability, leading to full system compromise.	8.1	More Details
CVE-2022-26861	Dell BIOS versions contain an Insecure Automated Optimization vulnerability. A local authenticated malicious user could exploit this vulnerability by sending malicious input via SMI to obtain arbitrary code execution during SMM.	7.9	More Details
CVE-2022-34382	Dell Command Update, Dell Update and Alienware Update versions prior to 4.6.0 contains a Local Privilege Escalation Vulnerability in the custom catalog configuration. A local malicious user may potentially exploit this vulnerability in order to elevate their privileges.	7.8	More Details
CVE-2022-3134	Use After Free in GitHub repository vim/vim prior to 9.0.0389.	7.8	More Details
CVE-2022-36041	Rizin is a UNIX-like reverse engineering framework and command-line toolset. Versions 0.4.0 and prior are vulnerable to an out-of-bounds write when parsing Mach-O files. A user opening a malicious Mach-O file could be affected by this vulnerability, allowing an attacker to execute code on the user's machine. Commit number 7323e64d68ecccfb0ed3ee480f704384c38676b2 contains a patch.	7.8	More Details
CVE-2022-36043	Rizin is a UNIX-like reverse engineering framework and command-line toolset. Versions 0.4.0 and prior are vulnerable to a double free in bobj.c:rz_bin_reloc_storage_free() when freeing relocations generated from qnx binary plugin. A user opening a malicious qnx binary could be affected by this vulnerability, allowing an attacker to execute code on the user's machine. Commit number a3d50c1ea185f3f642f2d8180715f82d98840784 contains a patch for this issue.	7.8	More Details
CVE-2022-36044	Rizin is a UNIX-like reverse engineering framework and command-line toolset. Versions 0.4.0 and prior are vulnerable to an out-of-bounds write when getting data from Luac files. A user opening a malicious Luac file could be affected by this vulnerability, allowing an attacker to execute code on the user's machine. Commits 07b43bc8aa1ffebd9b68d60624c9610cf7e460c7 and 05bbd147caccc60162d6fba9baaaf24befa281cd contain fixes for the issue.	7.8	More Details
CVE-2022-2639	An integer coercion error was found in the openvswitch kernel module. Given a sufficiently large number of actions, while copying and reserving memory for a new action of a new flow, the reserve_sfa_size() function does not return -EMSGSIZE as expected, potentially leading to an out-of-bounds write access. This flaw allows a local user to crash or potentially escalate their privileges on the system.	7.8	More Details
CVE-2021-25657	A privilege escalation vulnerability was discovered in Avaya IP Office Admin Lite and USB Creator that may potentially allow a local user to escalate privileges. This issue affects Admin Lite and USB Creator 11.1 Feature Pack 2 Service Pack 1 and earlier versions.	7.8	More Details
CVE-2022-38176	An issue was discovered in YSoft SAFEQ 6 before 6.0.72. Incorrect privileges were configured as part of the installer package for the Client V3 services, allowing for local user privilege escalation by overwriting the executable file via an alternative data stream. NOTE: this is not the same as CVE-2021-31859.	7.8	More Details
CVE-2022-36040	Rizin is a UNIX-like reverse engineering framework and command-line toolset. Versions 0.4.0 and prior are vulnerable to an out-of-bounds write when getting data from PYC(python) files. A user opening a malicious PYC file could be affected by this vulnerability, allowing an attacker to execute code on the user's machine. Commit number 68948017423a12786704e54227b8b2f918c2fd27 contains a patch.	7.8	More Details
CVE-2022-38529	tinyexr commit 0647fb3 was discovered to contain a heap-buffer overflow via the component rleUncompress.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2320	A flaw was found in the Xorg-x11-server. The specific flaw exists within the handling of ProcXkbSetDeviceInfo requests. The issue results from the lack of proper validation of user-supplied data, which can result in a memory access past the end of an allocated buffer. This flaw allows an attacker to escalate privileges and execute arbitrary code in the context of root.	7.8	More Details
CVE-2022-2319	A flaw was found in the Xorg-x11-server. An out-of-bounds access issue can occur in the ProcXkbSetGeometry function due to improper validation of the request length.	7.8	More Details
CVE-2022-39189	An issue was discovered the x86 KVM subsystem in the Linux kernel before 5.18.17. Unprivileged guest users can compromise the guest kernel because TLB flush operations are mishandled in certain KVM_VCPU_PREEMPTED situations.	7.8	More Details
CVE-2022-22061	Out of bounds writing is possible while verifying device IDs due to improper length check before copying the data in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile	7.8	More Details
CVE-2022-36042	Rizin is a UNIX-like reverse engineering framework and command-line toolset. Versions 0.4.0 and prior are vulnerable to an out-of-bounds write when getting data from dyld cache files. A user opening a malicious dyld cache file could be affected by this vulnerability, allowing an attacker to execute code on the user's machine. Commit number 556ca2f9eef01ec0f4a76d1fbacfcf3a87a44810 contains a patch.	7.8	More Details
CVE-2022-36039	Rizin is a UNIX-like reverse engineering framework and command-line toolset. Versions 0.4.0 and prior are vulnerable to out-of-bounds write when parsing DEX files. A user opening a malicious DEX file could be affected by this vulnerability, allowing an attacker to execute code on the user's machine. A patch is available on the `dev` branch of the repository.	7.8	More Details
CVE-2022-31791	WatchGuard Firebox and XTM appliances allow a local attacker (that has already obtained shell access) to elevate their privileges and execute code with root permissions. This is fixed in Fireware OS 12.8.1, 12.5.10, and 12.1.4.	7.8	More Details
CVE-2022-2735	A vulnerability was found in the PCS project. This issue occurs due to incorrect permissions on a Unix socket used for internal communication between PCS daemons. A privilege escalation could happen by obtaining an authentication token for a hacluster user. With the "hacluster" token, this flaw allows an attacker to have complete control over the cluster managed by PCS.	7.8	More Details
CVE-2022-22070	Memory corruption in audio due to lack of check of invalid routing address into APR Routing table in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.8	More Details
CVE-2022-29058	An improper neutralization of special elements [CWE-89] used in an OS command vulnerability [CWE-78] in the command line interpreter of FortiAP 6.0.0 through 6.4.7, 7.0.0 through 7.0.3, 7.2.0, FortiAP-S 6.0.0 through 6.4.7, FortiAP-W2 6.0.0 through 6.4.7, 7.0.0 through 7.0.3, 7.2.0 and FortiAP-U 5.4.0 through 6.2.3 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands.	7.8	More Details
CVE-2022-26469	In MtkEmail, there is a possible escalation of privilege due to fragment injection. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07216598; Issue ID: ALPS07216598.	7.8	More Details
CVE-2022-25308	A stack-based buffer overflow flaw was found in the Fribidi package. This flaw allows an attacker to pass a specially crafted file to the Fribidi application, which leads to a possible memory leak or a denial of service.	7.8	More Details
CVE-2022-23682	Multiple vulnerabilities exist in the AOS-CX command line interface that could lead to authenticated command injection. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete switch compromise in ArubaOS-CX version(s): AOS-CX 10.09.xxxx: 10.09.1030 and below, AOS-CX 10.08.xxxx: 10.08.1030 and below, AOS-CX 10.06.xxxx: 10.06.0180 and below. Aruba has released upgrades for ArubaOS-CX Switch Devices that address these security vulnerabilities.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23681	Multiple vulnerabilities exist in the AOS-CX command line interface that could lead to authenticated command injection. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete switch compromise in ArubaOS-CX version(s): AOS-CX 10.09.xxxx: 10.09.1030 and below, AOS-CX 10.08.xxxx: 10.08.1030 and below, AOS-CX 10.06.xxxx: 10.06.0180 and below. Aruba has released upgrades for ArubaOS-CX Switch Devices that address these security vulnerabilities.	7.8	More Details
CVE-2022-39843	123elf Lotus 1-2-3 before 1.0.0rc3 for Linux, and Lotus 1-2-3 R3 for UNIX and other platforms through 9.8.2, allow attackers to execute arbitrary code via a crafted worksheet. This occurs because of a stack-based buffer overflow in the cell format processing routines, as demonstrated by a certain function call from process_fmt() that can be reached via a w3r_format element in a wk3 document.	7.8	More Details
CVE-2022-39831	An issue was discovered in PSPP 1.6.2. There is a heap-based buffer overflow at the function read_bytes_internal in utilities/pspp-dump-sav.c, which allows attackers to cause a denial of service (application crash) or possibly have unspecified other impact. This issue is different from CVE-2018-20230.	7.8	More Details
CVE-2022-3099	Use After Free in GitHub repository vim/vim prior to 9.0.0360.	7.8	More Details
CVE-2022-39832	An issue was discovered in PSPP 1.6.2. There is a heap-based buffer overflow at the function read_string in utilities/pspp-dump-sav.c, which allows attackers to cause a denial of service (application crash) or possibly have unspecified other impact.	7.8	More Details
CVE-2022-38530	GPAC v2.1-DEV-rev232-gfcaa01ebb-master was discovered to contain a stack overflow when processing ISOM_IOD.	7.8	More Details
CVE-2022-2896	Measuresoft ScadaPro Server (All Versions) allows use after free while processing a specific project file.	7.8	More Details
CVE-2022-2006	AutomationDirect DirectLOGIC has a DLL vulnerability in the install directory that may allow an attacker to execute code during the installation process. This issue affects: AutomationDirect C-more EA9 EA9-T6CL versions prior to 6.73; EA9-T6CL-R versions prior to 6.73; EA9-T7CL versions prior to 6.73; EA9-T7CL-R versions prior to 6.73; EA9-T8CL versions prior to 6.73; EA9-T10CL versions prior to 6.73; EA9-T10WCL versions prior to 6.73; EA9-T12CL versions prior to 6.73; EA9-T15CL versions prior to 6.73; EA9-RHMI versions prior to 6.73; EA9-PGMSW versions prior to 6.73;	7.8	More Details
CVE-2022-2866	FATEK FvDesigner version 1.5.103 and prior is vulnerable to an out-of-bounds write while processing project files. If a valid user is tricked into using maliciously crafted project files, an attacker could achieve arbitrary code execution.	7.8	More Details
CVE-2022-2897	Measuresoft ScadaPro Server and Client (All Versions) do not properly resolve links before file access; this could allow privilege escalation..	7.8	More Details
CVE-2022-1888	Alpha7 PC Loader (All versions) is vulnerable to a stack-based buffer overflow while processing a specifically crafted project file, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2022-1976	A flaw was found in the Linux kernel's implementation of IO-URING. This flaw allows an attacker with local executable permission to create a string of requests that can cause a use-after-free flaw within the kernel. This issue leads to memory corruption and possible privilege escalation.	7.8	More Details
CVE-2022-2892	Measuresoft ScadaPro Server (Versions prior to 6.8.0.1) uses an unmaintained ActiveX control, which may allow an out-of-bounds write condition while processing a specific project file.	7.8	More Details
CVE-2022-2894	Measuresoft ScadaPro Server (All Versions) uses unmaintained ActiveX controls. The controls may allow seven untrusted pointer deference instances while processing a specific project file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1405	CNCSoft: All versions prior to 1.01.32 does not properly sanitize input while processing a specific project file, allowing a possible stack-based buffer overflow condition.	7.8	More Details
CVE-2022-2895	Measuresoft ScadaPro Server (All Versions) uses unmaintained ActiveX controls. These controls may allow two stack-based buffer overflow instances while processing a specific project file.	7.8	More Details
CVE-2022-2003	AutomationDirect DirectLOGIC is vulnerable to a specifically crafted serial message to the CPU serial port that will cause the PLC to respond with the PLC password in cleartext. This could allow an attacker to access and make unauthorized changes. This issue affects: AutomationDirect DirectLOGIC D0-06 series CPUs D0-06DD1 versions prior to 2.72; D0-06DD2 versions prior to 2.72; D0-06DR versions prior to 2.72; D0-06DA versions prior to 2.72; D0-06AR versions prior to 2.72; D0-06AA versions prior to 2.72; D0-06DD1-D versions prior to 2.72; D0-06DD2-D versions prior to 2.72; D0-06DR-D versions prior to 2.72;	7.7	More Details
CVE-2022-36035	Flux is a tool for keeping Kubernetes clusters in sync with sources of configuration (like Git repositories), and automating updates to configuration when there is new code to deploy. Flux CLI allows users to deploy Flux components into a Kubernetes cluster via command-line. The vulnerability allows other applications to replace the Flux deployment information with arbitrary content which is deployed into the target Kubernetes cluster instead. The vulnerability is due to the improper handling of user-supplied input, which results in a path traversal that can be controlled by the attacker. Users sharing the same shell between other applications and the Flux CLI commands could be affected by this vulnerability. In some scenarios no errors may be presented, which may cause end users not to realize that something is amiss. A safe workaround is to execute Flux CLI in ephemeral and isolated shell environments, which can ensure no persistent values exist from previous processes. However, upgrading to the latest version of the CLI is still the recommended mitigation strategy.	7.7	More Details
CVE-2022-22069	Devices with keyprotect off may store unencrypted keybox in RPMB and cause cryptographic issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	7.7	More Details
CVE-2022-36387	Broken Access Control vulnerability in Alessio Caiazza's About Me plugin <= 1.0.12 at WordPress.	7.6	More Details
CVE-2022-37344	Missing Access Control vulnerability in PHP Crafts Accommodation System plugin <= 1.0.1 at WordPress.	7.6	More Details
CVE-2022-31196	Databasir is a database metadata management platform. Databasir <= 1.06 has Server-Side Request Forgery (SSRF) vulnerability. The SSRF is triggered by a sending a **single** HTTP POST request to create a databaseType. By supplying a `jdbcDriverFileUrl` that returns a non `200` response code, the url is executed, the response is logged (both in terminal and in database) and is included in the response. This would allow an attackers to obtain the real IP address and scan Intranet information. This issue was fixed in version 1.0.7.	7.6	More Details
CVE-2022-39829	There is a NULL pointer dereference in aes256_encrypt in Samsung mTower through 0.3.0 due to a missing check on the return value of EVP_CIPHER_CTX_new.	7.5	More Details
CVE-2022-36622	Samsung Electronics mTower v0.3.0 and earlier was discovered to contain a NULL pointer dereference via the function TEE_GetObjectInfo1.	7.5	More Details
CVE-2022-36621	Samsung Electronics mTower v0.3.0 and earlier was discovered to contain a NULL pointer dereference via the function TEE_AllocateTransientObject.	7.5	More Details
CVE-2022-36604	An access control issue in Canaan Avalon ASIC Miner 2020.3.30 and below allows unauthenticated attackers to arbitrarily change user passwords via a crafted POST request.	7.5	More Details
CVE-2022-36619	In D-link DIR-816 A2_v1.10CNB04.img,the network can be reset without authentication via /goform/setMAC.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39830	sign_pFwInfo in Samsung mTower through 0.3.0 has a missing check on the return value of EC_KEY_set_public_key_affine_coordinates, leading to a denial of service.	7.5	More Details
CVE-2022-22067	Potential memory leak in modem during the processing of NSA RRC Reconfiguration with invalid Radio Bearer Config in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile	7.5	More Details
CVE-2022-38152	An issue was discovered in wolfSSL before 5.5.0. When a TLS 1.3 client connects to a wolfSSL server and SSL_clear is called on its session, the server crashes with a segmentation fault. This occurs in the second session, which is created through TLS session resumption and reuses the initial struct WOLFSSL. If the server reuses the previous session structure (struct WOLFSSL) by calling wolfSSL_clear(WOLFSSL* ssl) on it, the next received Client Hello (that resumes the previous session) crashes the server. Note that this bug is only triggered when resuming sessions using TLS session resumption. Only servers that use wolfSSL_clear instead of the recommended SSL_free; SSL_new sequence are affected. Furthermore, wolfSSL_clear is part of wolfSSL's compatibility layer and is not enabled by default. It is not part of wolfSSL's native API.	7.5	More Details
CVE-2022-1259	A flaw was found in Undertow. A potential security issue in flow control handling by the browser over HTTP/2 may cause overhead or a denial of service in the server. This flaw exists because of an incomplete fix for CVE-2021-3629.	7.5	More Details
CVE-2022-1319	A flaw was found in Undertow. For an AJP 400 response, EAP 7 is improperly sending two response packets, and those packets have the reuse flag set even though JBoss EAP closes the connection. A failure occurs when the connection is reused after a 400 by CPING since it reads in the second SEND_HEADERS response packet instead of a CPONG.	7.5	More Details
CVE-2020-29260	libvncclient v0.9.13 was discovered to contain a memory leak via the function rfbClientCleanup().	7.5	More Details
CVE-2022-39828	sign_pFwInfo in Samsung mTower through 0.3.0 has a missing check on the return value of EC_KEY_set_private_key, leading to a denial of service.	7.5	More Details
CVE-2022-36620	D-link DIR-816 A2_v1.10CNB04, DIR-878 DIR_878_FW1.30B08.img is vulnerable to Buffer Overflow via /goform/addRouting.	7.5	More Details
CVE-2022-2633	The All-in-One Video Gallery plugin for WordPress is vulnerable to arbitrary file downloads and blind server-side request forgery via the 'dl' parameter found in the ~/public/video.php file in versions up to, and including 2.6.0. This makes it possible for unauthenticated users to download sensitive files hosted on the affected server and forge requests to the server.	7.5	More Details
CVE-2022-3065	Improper Access Control in GitHub repository jgraph/drawio prior to 20.2.8.	7.5	More Details
CVE-2022-2738	The version of podman as released for Red Hat Enterprise Linux 7 Extras via RHSA-2022:2190 advisory included an incorrect version of podman missing the fix for CVE-2020-8945, which was previously fixed via RHSA-2020:2117. This issue could possibly be used to crash or cause potential code execution in Go applications that use the Go GPGME wrapper library, under certain conditions, during GPG signature verification.	7.5	More Details
CVE-2022-31790	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to retrieve sensitive authentication server settings by sending a malicious request to exposed authentication endpoints. This is fixed in Fireware OS 12.8.1, 12.5.10, and 12.1.4.	7.5	More Details
CVE-2022-25813	In Apache OFBiz, versions 18.12.05 and earlier, an attacker acting as an anonymous user of the ecommerce plugin, can insert a malicious content in a message “Subject” field from the "Contact us" page. Then a party manager needs to list the communications in the party component to activate the SSTI. A RCE is then possible.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29158	Apache OFBiz up to version 18.12.05 is vulnerable to Regular Expression Denial of Service (ReDoS) in the way it handles URLs provided by external, unauthenticated users. Upgrade to 18.12.06 or apply patches at https://issues.apache.org/jira/browse/OFBIZ-12599	7.5	More Details
CVE-2022-36671	Novel-Plus v3.6.2 was discovered to contain an arbitrary file download vulnerability via the background file download API.	7.5	More Details
CVE-2022-36581	Online Ordering System v2.3.2 was discovered to contain a SQL injection vulnerability via the user_email parameter at /admin/login.php.	7.5	More Details
CVE-2022-32264	sys/netinet/tcp_timer.h in FreeBSD before 7.0 contains a denial-of-service (DoS) vulnerability due to improper handling of TSopt on TCP connections. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	7.5	More Details
CVE-2022-39046	An issue was discovered in the GNU C Library (glibc) 2.36. When the syslog function is passed a crafted input string larger than 1024 bytes, it reads uninitialized memory from the heap and prints it to the target log file, potentially revealing a portion of the contents of the heap.	7.5	More Details
CVE-2022-37122	Carel pCOWeb HVAC BACnet Gateway 2.1.0, Firmware: A2.1.0 - B2.1.0, Application Software: 2.15.4A Software v16 13020200 suffers from an unauthenticated arbitrary file disclosure vulnerability. Input passed through the 'file' GET parameter through the 'logdownload.cgi' Bash script is not properly verified before being used to download log files. This can be exploited to disclose the contents of arbitrary and sensitive files via directory traversal attacks.	7.5	More Details
CVE-2022-37841	In TOTOLINK A860R V4.1.2cu.5182_B20201027 there is a hard coded password for root in /etc/shadow.sample.	7.5	More Details
CVE-2022-2004	AutomationDirect DirectLOGIC is vulnerable to a a specially crafted packet can be sent continuously to the PLC to prevent access from DirectSoft and other devices, causing a denial-of-service condition. This issue affects: AutomationDirect DirectLOGIC D0-06 series CPUs D0-06DD1 versions prior to 2.72; D0-06DD2 versions prior to 2.72; D0-06DR versions prior to 2.72; D0-06DA versions prior to 2.72; D0-06AR versions prior to 2.72; D0-06AA versions prior to 2.72; D0-06DD1-D versions prior to 2.72; D0-06DD2-D versions prior to 2.72; D0-06DR-D versions prior to 2.72;	7.5	More Details
CVE-2022-2005	AutomationDirect C-more EA9 HTTP webserver uses an insecure mechanism to transport credentials from client to web server, which may allow an attacker to obtain the login credentials and login as a valid user. This issue affects: AutomationDirect C-more EA9 EA9-T6CL versions prior to 6.73; EA9-T6CL-R versions prior to 6.73; EA9-T7CL versions prior to 6.73; EA9-T7CL-R versions prior to 6.73; EA9-T8CL versions prior to 6.73; EA9-T10CL versions prior to 6.73; EA9-T10WCL versions prior to 6.73; EA9-T12CL versions prior to 6.73; EA9-T15CL versions prior to 6.73; EA9-RHMI versions prior to 6.73; EA9-PGMSW versions prior to 6.73;	7.5	More Details
CVE-2022-36065	GrowthBook is an open-source platform for feature flagging and A/B testing. With some self-hosted configurations in versions prior to 2022-08-29, attackers can register new accounts and upload files to arbitrary directories within the container. If the attacker uploads a Python script to the right location, they can execute arbitrary code within the container. To be affected, ALL of the following must be true: Self-hosted deployment (GrowthBook Cloud is unaffected); using local file uploads (as opposed to S3 or Google Cloud Storage); NODE_ENV set to a non-production value and JWT_SECRET set to an easily guessable string like `dev`. This issue is patched in commit 1a5edff8786d141161bf880c2fd9ccbe2850a264 (2022-08-29). As a workaround, set `JWT_SECRET` environment variable to a long random string. This will stop arbitrary file uploads, but the only way to stop attackers from registering accounts is by updating to the latest build.	7.5	More Details
CVE-2022-2043	MOXA NPort 5110: Firmware Versions 2.10 is vulnerable to an out-of-bounds write that can cause the device to become unresponsive.	7.5	More Details
CVE-2021-45027	An arbitrary file download vulnerability in Oliver v5 Library Server Versions < 5.00.008.053 via the FileServlet function allows for arbitrary file download by an attacker using unsanitized user supplied input.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27664	In net/http in Go before 1.18.6 and 1.19.x before 1.19.1, attackers can cause a denial of service because an HTTP/2 connection can hang during closing if shutdown were preempted by a fatal error.	7.5	More Details
CVE-2021-43565	The x/crypto/ssh package before 0.0.0-20211202192323-5770296d904e of golang.org/x/crypto allows an attacker to panic an SSH server.	7.5	More Details
CVE-2022-40112	TOTOLINK A3002R TOTOLINK-A3002R-He-V1.1.1-B20200824.0128 is vulnerable Buffer Overflow via the hostname parameter in binary /bin/boa.	7.5	More Details
CVE-2022-26860	Dell BIOS versions contain a stack-based buffer overflow vulnerability. A local attacker could exploit this vulnerability by sending malicious input via SMI to bypass security checks resulting in arbitrary code execution in SMM.	7.5	More Details
CVE-2022-40110	TOTOLINK A3002R TOTOLINK-A3002R-He-V1.1.1-B20200824.0128 is vulnerable to Buffer Overflow via /bin/boa.	7.5	More Details
CVE-2022-30614	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.2.1 is vulnerable to a denial of service via email flooding caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume all available CPU resources. IBM X-Force ID: 227591.	7.5	More Details
CVE-2022-32743	Samba does not validate the Validated-DNS-Host-Name right for the dNSHostName attribute which could permit unprivileged users to write it.	7.5	More Details
CVE-2022-36058	Elrond go is the go implementation for the Elrond Network protocol. In versions prior to 1.3.34, anyone who uses elrond-go to process blocks (historical or actual) could encounter a `MultiESDTNFTTransfer` transaction like this: `MultiESDTNFTTransfer` with a missing function name. Basic functionality like p2p messaging, storage, API requests and such are unaffected. Version 1.3.34 contains a fix for this issue. There are no known workarounds.	7.5	More Details
CVE-2022-38370	Apache IoTDB grafana-connector version 0.13.0 contains an interface without authorization, which may expose the internal structure of database. Users should upgrade to version 0.13.1 which addresses this issue.	7.5	More Details
CVE-2022-2083	The Simple Single Sign On WordPress plugin through 4.1.0 leaks its OAuth client_secret, which could be used by attackers to gain unauthorized access to the site.	7.5	More Details
CVE-2022-37185	SQL injection vulnerability exists in the school information query interface (repschoolproj.php) of the EMS 6.2 system of the Office of the Thai Basic Education Commission, which can lead to data leakage.	7.5	More Details
CVE-2020-35525	In SQlite 3.31.1, a potential null pointer derreference was found in the INTERSEC query processing.	7.5	More Details
CVE-2022-2996	A flaw was found in the python-scciclient when making an HTTPS connection to a server where the server's certificate would not be verified. This issue opens up the connection to possible Man-in-the-middle (MITM) attacks.	7.4	More Details
CVE-2022-25659	Memory corruption due to buffer overflow while parsing MKV clips with invalid bitmap size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.3	More Details
CVE-2021-35113	Possible authentication bypass due to improper order of signature verification and hashing in the signature verification call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25657	Memory corruption due to buffer overflow occurs while processing invalid MKV clip which has invalid seek header in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	7.3	More Details
CVE-2021-35097	Possible authentication bypass due to improper order of signature verification and hashing in the signature verification call in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.3	More Details
CVE-2022-25658	Memory corruption due to incorrect pointer arithmetic when attempting to change the endianness in video parser function in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.3	More Details
CVE-2022-3120	A vulnerability classified as critical was found in SourceCodester Clinics Patient Management System. Affected by this vulnerability is an unknown functionality of the file index.php of the component Login. The manipulation of the argument user_name leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-207847.	7.3	More Details
CVE-2022-34373	Dell Command | Integration Suite for System Center, versions prior to 6.2.0, contains arbitrary file write vulnerability. A locally authenticated malicious user could potentially exploit this vulnerability in order to perform an arbitrary write as system.	7.3	More Details
CVE-2022-3118	A vulnerability was found in Sourcecodehero ERP System Project. It has been rated as critical. This issue affects some unknown processing of the file /pages/processlogin.php. The manipulation of the argument user leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-207845 was assigned to this vulnerability.	7.3	More Details
CVE-2022-36427	Missing Access Control vulnerability in About Rentals. Inc. About Rentals plugin <= 1.5 at WordPress.	7.3	More Details
CVE-2022-34867	Unauthenticated Sensitive Information Disclosure vulnerability in WP Libre Form 2 plugin <= 2.0.8 at WordPress allows attackers to list and delete submissions. Affects only versions from 2.0.0 to 2.0.8.	7.3	More Details
CVE-2022-25668	Memory corruption in video driver due to double free while parsing ASF clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.3	More Details
CVE-2022-36582	An arbitrary file upload vulnerability in the component /php_action/createProduct.php of Garage Management System v1.0 allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details
CVE-2022-2442	The Migration, Backup, Staging – WPvivid plugin for WordPress is vulnerable to deserialization of untrusted input via the 'path' parameter in versions up to, and including 0.9.74. This makes it possible for authenticated attackers with administrative privileges to call files using a PHAR wrapper that will deserialize and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.	7.2	More Details
CVE-2022-23683	Authenticated command injection vulnerabilities exist in the AOS-CX Network Analytics Engine via NAE scripts. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX in ArubaOS-CX Switches version(s): AOS-CX 10.10.xxxx: 10.10.0002 and below, AOS-CX 10.09.xxxx: 10.09.1030 and below, AOS-CX 10.08.xxxx: 10.08.1070 and below, AOS-CX 10.06.xxxx: 10.06.0210 and below. Aruba has released upgrades for ArubaOS-CX Switch Devices that address these security vulnerabilities.	7.2	More Details
CVE-2022-2565	The Simple Payment Donations & Subscriptions WordPress plugin before 4.2.1 does not sanitise and escape user input given in its forms, which could allow unauthenticated attackers to perform Cross-Site Scripting attacks against admins	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2438	The Broken Link Checker plugin for WordPress is vulnerable to deserialization of untrusted input via the '$log_file' value in versions up to, and including 1.11.16. This makes it possible for authenticated attackers with administrative privileges and above to call files using a PHAR wrapper that will deserialize the data and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.	7.2	More Details
CVE-2022-34883	OS Command Injection vulnerability in Hitachi RAID Manager Storage Replication Adapter allows remote authenticated users to execute arbitrary OS commands. This issue affects: Hitachi RAID Manager Storage Replication Adapter 02.01.04 versions prior to 02.03.02 on Windows; 02.05.00 versions prior to 02.05.01 on Windows and Docker.	7.2	More Details
CVE-2022-36580	An arbitrary file upload vulnerability in the component /admin/products/controller.php?action=add of Online Ordering System v2.3.2 allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details
CVE-2021-28398	A privileged attacker in GeoNetwork before 3.12.0 and 4.x before 4.0.4 can use the directory harvester before-script to execute arbitrary OS commands remotely on the hosting infrastructure. A User Administrator or Administrator account is required to perform this. This occurs in the runBeforeScript method in harvesters/src/main/java/org/fao/geonet/kernel/harvest/harvester/localfilesystem/LocalFilesystemHarvester.java. The earliest affected version is 3.4.0.	7.2	More Details
CVE-2022-36571	Tenda AC9 V15.03.05.19 was discovered to contain a stack overflow via the mask parameter at /goform/WanParameterSetting.	7.2	More Details
CVE-2022-37458	Discourse through 2.8.7 allows admins to send invitations to arbitrary email addresses at an unlimited rate.	7.2	More Details
CVE-2022-2717	The JoomSport – for Sports: Team & League, Football, Hockey & more plugin for WordPress is vulnerable to SQL Injection via the 'orderby' parameter on the joomsport-events-form page in versions up to, and including, 5.2.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrative privileges, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.2	More Details
CVE-2022-36754	Expense Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /Home/debit_credit_p.	7.2	More Details
CVE-2022-1841	In subsys/net/ip/tcp.c , function tcp_flags , when the incoming parameter flags is ECN or CWR , the buf will out-of-bounds write a byte zero.	7.2	More Details
CVE-2022-2718	The JoomSport – for Sports: Team & League, Football, Hockey & more plugin for WordPress is vulnerable to SQL Injection via the 'orderby' parameter on the joomsport-page-extrafields page in versions up to, and including, 5.2.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrative privileges, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.2	More Details
CVE-2022-36570	Tenda AC9 V15.03.05.19 was discovered to contain a stack overflow via the time parameter at /goform/SetLEDCfg.	7.2	More Details
CVE-2022-36674	Simple Task Scheduling System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /schedules/view_schedule.php.	7.2	More Details
CVE-2022-36676	Simple Task Scheduling System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /categories/view_category.php.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36675	Simple Task Scheduling System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /schedules/manage_schedule.php.	7.2	More Details
CVE-2022-2901	Improper Authorization in GitHub repository chatwoot/chatwoot prior to 2.8.	7.1	More Details
CVE-2022-1247	An issue found in linux-kernel that leads to a race condition in rose_connect(). The rose driver uses rose_neigh->use to represent how many objects are using the rose_neigh. When a user wants to delete a rose_route via rose_ioctl(), the rose driver calls rose_del_node() and removes neighbours only if their “count” and “use” are zero.	7.0	More Details
CVE-2022-1729	A race condition was found the Linux kernel in perf_event_open() which can be exploited by an unprivileged user to gain root privileges. The bug allows to build several exploit primitives such as kernel address information leak, arbitrary execution, etc.	7.0	More Details
CVE-2022-2590	A race condition was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only shared memory mappings. This flaw allows an unprivileged, local user to gain write access to read-only memory mappings, increasing their privileges on the system.	7.0	More Details
CVE-2022-30298	An improper privilege management vulnerability [CWE-269] in Fortinet FortiSOAR before 7.2.1 allows a GUI user who has already found a way to modify system files (via another, unrelated and hypothetical exploit) to execute arbitrary Python commands as root.	7.0	More Details
CVE-2022-3028	A race condition was found in the Linux kernel's IP framework for transforming packets (XFRM subsystem) when multiple calls to xfrm_probe_algs occurred simultaneously. This flaw could allow a local attacker to potentially trigger an out-of-bounds write or leak kernel heap memory by performing an out-of-bounds read and copying it into a socket.	7.0	More Details
CVE-2022-27491	A improper verification of source of a communication channel in Fortinet FortiOS with IPS engine version 7.201 through 7.214, 7.001 through 7.113, 6.001 through 6.121, 5.001 through 5.258 and before 4.086 allows a remote and unauthenticated attacker to trigger the sending of "blocked page" HTML data to an arbitrary victim via crafted TCP requests, potentially flooding the victim.	6.8	More Details
CVE-2022-23691	A vulnerability exists in certain AOS-CX switch models which could allow an attacker with access to the recovery console to bypass normal authentication. A successful exploit allows an attacker to bypass system authentication and achieve total switch compromise in ArubaOS-CX Switches version(s): AOS-CX 10.10.xxxx: 10.10.0002 and below, AOS-CX 10.09.xxxx: 10.09.1030 and below, AOS-CX 10.08.xxxx: 10.08.1070 and below, AOS-CX 10.06.xxxx: 10.06.0210 and below. Aruba has released upgrades for ArubaOS-CX Switch Devices that address this security vulnerability.	6.8	More Details
CVE-2021-35108	Improper checking of AP-S lock bit while verifying the secure resource group permissions can lead to non secure read and write access in Snapdragon Connectivity, Snapdragon Mobile	6.8	More Details
CVE-2022-39051	Attacker might be able to execute malicious Perl code in the Template toolkit, by having the admin installing an unverified 3th party package	6.8	More Details
CVE-2022-36054	Contiki-NG is an open-source, cross-platform operating system for Next-Generation IoT devices. The 6LoWPAN implementation in the Contiki-NG operating system (file os/net/ipv6/sicslowpan.c) contains an input function that processes incoming packets and copies them into a packet buffer. Because of a missing length check in the input function, it is possible to write outside the packet buffer's boundary. The vulnerability can be exploited by anyone who has the possibility to send 6LoWPAN packets to a Contiki-NG system. In particular, the vulnerability is exposed when sending either of two types of 6LoWPAN packets: an unfragmented packet or the first fragment of a fragmented packet. If the packet is sufficiently large, a subsequent memory copy will cause an out-of-bounds write with data supplied by the attacker.	6.8	More Details
CVE-2021-35109	Possible address manipulation from APP-NS while APP-S is configuring an RG where it tries to merge the address ranges in Snapdragon Connectivity, Snapdragon Mobile	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26458	In vow, 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: ALPS07032678; Issue ID: ALPS07032678.	6.7	More Details
CVE-2022-36670	PCProtect Endpoint prior to v5.17.470 for Microsoft Windows lacks tamper protection, allowing authenticated attackers with Administrator privileges to modify processes within the application and escalate privileges to SYSTEM via a crafted executable.	6.7	More Details
CVE-2022-37771	IObit Malware Fighter v9.2 for Microsoft Windows lacks tamper protection, allowing authenticated attackers with Administrator privileges to modify processes within the application and escalate privileges to SYSTEM via a crafted executable.	6.7	More Details
CVE-2022-26454	In teei, there is a possible memory corruption 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. Patch ID: ALPS06664701; Issue ID: ALPS06664701.	6.7	More Details
CVE-2022-26453	In teei, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06664675; Issue ID: ALPS06664675.	6.7	More Details
CVE-2022-26451	In ged, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07202966; Issue ID: ALPS07202966.	6.7	More Details
CVE-2022-26449	In apusys, 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: ALPS07177810; Issue ID: ALPS07177810.	6.7	More Details
CVE-2022-26470	In aie, 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: ALPS07116037; Issue ID: ALPS07116037.	6.7	More Details
CVE-2022-26467	In rpmb, 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: ALPS07167738; Issue ID: ALPS07167738.	6.7	More Details
CVE-2022-26460	In vow, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032590; Issue ID: ALPS07032590.	6.7	More Details
CVE-2022-26448	In apusys, 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: ALPS07063849; Issue ID: ALPS07063849.	6.7	More Details
CVE-2022-26466	In audio ipi, 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. Patch ID: ALPS06558777; Issue ID: ALPS06558777.	6.7	More Details
CVE-2022-26464	In vow, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032699; Issue ID: ALPS07032699.	6.7	More Details
CVE-2022-26461	In vow, there is a possible undefined behavior due to an API misuse. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032604; Issue ID: ALPS07032604.	6.7	More Details
CVE-2022-26465	In audio ipi, 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: ALPS06558799; Issue ID: ALPS06558799.	6.7	More Details
CVE-2022-26455	In gz, there is a possible memory corruption due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07177858; Issue ID: ALPS07177858.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26457	In vow, 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: ALPS07138490; Issue ID: ALPS07138490.	6.7	More Details
CVE-2021-35133	Use after free in the synx driver issue while performing other functions during multiple invocation of synx release calls in Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	6.7	More Details
CVE-2022-26468	In preloader (usb), there is a possible out of bounds write due to a missing bounds check. 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 needed for exploitation. Patch ID: ALPS07168125; Issue ID: ALPS07168125.	6.6	More Details
CVE-2022-2447	A flaw was found in Keystone. There is a time lag (up to one hour in a default configuration) between when security policy says a token should be revoked from when it is actually revoked. This could allow a remote administrator to secretly maintain access for longer than expected.	6.6	More Details
CVE-2021-3826	Heap/stack buffer overflow in the dlang_lname function in d-demangle.c in libiberty allows attackers to potentially cause a denial of service (segmentation fault and crash) via a crafted mangled symbol.	6.5	More Details
CVE-2021-20468	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.2.1 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: 196825.	6.5	More Details
CVE-2022-2308	A flaw was found in vDPA with VDUSE backend. There are currently no checks in VDUSE kernel driver to ensure the size of the device config space is in line with the features advertised by the VDUSE userspace application. In case of a mismatch, Virtio drivers config read helpers do not initialize the memory indirectly passed to vduse_vdpa_get_config() returning uninitialized memory from the stack. This could cause undefined behavior or data leaks in Virtio drivers.	6.5	More Details
CVE-2022-38528	Open Asset Import Library (assimp) commit 3c253ca was discovered to contain a segmentation violation via the component Assimp::XFileImporter::CreateMeshes.	6.5	More Details
CVE-2022-2238	A vulnerability was found in the search-api container in Red Hat Advanced Cluster Management for Kubernetes when a query in the search filter gets parsed by the backend. This flaw allows an attacker to craft specific strings containing special characters that lead to crashing the pod and affects system availability while restarting.	6.5	More Details
CVE-2022-38812	AeroCMS 0.1.1 is vulnerable to SQL Injection via the author parameter.	6.5	More Details
CVE-2022-36061	Elrond go is the go implementation for the Elrond Network protocol. In versions prior to 1.3.35, read only calls between contracts can generate smart contracts results. For example, if contract A calls in read only mode contract B and the called function will make changes upon the contract's B state, the state will be altered for contract B as if the call was not made in the read-only mode. This can lead to some effects not designed by the original smart contracts programmers. This issue was patched in version 1.3.35. There are no known workarounds.	6.5	More Details
CVE-2022-1632	An Improper Certificate Validation attack was found in Openshift. A re-encrypt Route with destinationCACertificate explicitly set to the default serviceCA skips internal Service TLS certificate validation. This flaw allows an attacker to exploit an invalid certificate, resulting in a loss of confidentiality.	6.5	More Details
CVE-2022-2521	It was found in libtiff 4.4.0rc1 that there is an invalid pointer free operation in TIFFClose() at tif_close.c:131 called by tiffcrop.c:2522 that can cause a program crash and denial of service while processing crafted input.	6.5	More Details
CVE-2022-38752	Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stack-overflow.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26330	Potential vulnerabilities have been identified in Micro Focus ArcSight Logger. The vulnerabilities could be remotely exploited resulting in Information Disclosure, or Self Cross-Site Scripting (XSS). This issue affects: Micro Focus ArcSight Logger versions prior to v7.2.2 version and prior versions.	6.5	More Details
CVE-2022-3026	The WP Users Exporter plugin for WordPress is vulnerable to CSV Injection in versions up to, and including, 1.4.2 via the 'Export Users' functionality. This makes it possible for authenticated attackers, such as a subscriber, to add untrusted input into profile information like First Names that will embed into the exported CSV file triggered by an administrator and can result in code execution when these files are downloaded and opened on a local system with a vulnerable configuration.	6.5	More Details
CVE-2022-2519	There is a double free or corruption in rotateImage() at tiffcrop.c:8839 found in libtiff 4.4.0rc1	6.5	More Details
CVE-2022-2429	The Ultimate SMS Notifications for WooCommerce plugin for WordPress is vulnerable to CSV Injection in versions up to, and including, 1.4.1 via the 'Export Utility' functionality. This makes it possible for authenticated attackers, such as a subscriber, to add untrusted input into billing information like their First Name that will embed into the exported CSV file triggered by an administrator and can result in code execution when these files are downloaded and opened on a local system with a vulnerable configuration.	6.5	More Details
CVE-2022-2520	A flaw was found in libtiff 4.4.0rc1. There is a sysmalloc assertion fail in rotateImage() at tiffcrop.c:8621 that can cause program crash when reading a crafted input.	6.5	More Details
CVE-2022-36593	kkFileView v4.0.0 was discovered to contain an arbitrary file deletion vulnerability via the fileName parameter at /controller/FileController.java.	6.5	More Details
CVE-2021-29823	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.2.1 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: 204465.	6.5	More Details
CVE-2022-2402	The vulnerability in the driver dlpfde.sys enables a user logged into the system to perform system calls leading to kernel stack overflow, resulting in a system crash, for instance, a BSOD.	6.5	More Details
CVE-2022-2758	Passwords are not adequately encrypted during the communication process between all versions of LS Industrial Systems (LSIS) Co. Ltd LS Electric XG5000 software prior to V4.0 and LS Electric PLCs: all versions of XGK-CPUU/H/A/S/E prior to V3.50, all versions of XGI-CPUU/UD/H/S/E prior to V3.20, all versions of XGR-CPUH prior to V1.80, all versions of XGB-XBMS prior to V3.00, all versions of XGB-XBCH prior to V1.90, and all versions of XGB-XECH prior to V1.30. This would allow an attacker to identify and decrypt the password of the affected PLCs by sniffing the PLC’s communication traffic.	6.5	More Details
CVE-2020-4301	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.2.1 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: 176609.	6.5	More Details
CVE-2022-37023	Apache Geode versions prior to 1.15.0 are vulnerable to a deserialization of untrusted data flaw when using REST API on Java 8 or Java 11. Any user wishing to protect against deserialization attacks involving REST APIs should upgrade to Apache Geode 1.15 and follow the documentation for details on enabling "validate-serializable-objects=true" and specifying any user classes that may be serialized/deserialized with "serializable-object-filter". Enabling "validate-serializable-objects" may impact performance.	6.5	More Details
CVE-2022-2403	A credentials leak was found in the OpenShift Container Platform. The private key for the external cluster certificate was stored incorrectly in the oauth-serving-cert ConfigMaps, and accessible to any authenticated OpenShift user or service-account. A malicious user could exploit this flaw by reading the oauth-serving-cert ConfigMap in the openshift-config-managed namespace, compromising any web traffic secured using that certificate.	6.5	More Details
CVE-2022-36449	An issue was discovered in the Arm Mali GPU Kernel Driver. A non-privileged user can make improper GPU processing operations to gain access to already freed memory, write a limited amount outside of buffer bounds, or to disclose details of memory mappings. This affects Midgard r4p0 through r32p0, Bifrost r0p0 through r38p0 and r39p0 before r38p1, and Valhall r19p0 through r38p0 and r39p0 before r38p1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39196	Blackboard Learn 1.10.1 allows remote authenticated users to read unintended files by entering student credentials and then directly visiting a certain webapps/bbcms/execute/ URL. Note: The vendor disputes this stating this cannot be reproduced.	6.5	More Details
CVE-2022-38751	Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow.	6.5	More Details
CVE-2022-36055	Helm is a tool for managing Charts. Charts are packages of pre-configured Kubernetes resources. Fuzz testing, provided by the CNCF, identified input to functions in the _strvals_ package that can cause an out of memory panic. The _strvals_ package contains a parser that turns strings in to Go structures. The _strvals_ package converts these strings into structures Go can work with. Some string inputs can cause array data structures to be created causing an out of memory panic. Applications that use the _strvals_ package in the Helm SDK to parse user supplied input can suffer a Denial of Service when that input causes a panic that cannot be recovered from. The Helm Client will panic with input to `--set`, `--set-string`, and other value setting flags that causes an out of memory panic. Helm is not a long running service so the panic will not affect future uses of the Helm client. This issue has been resolved in 3.9.4. SDK users can validate strings supplied by users won't create large arrays causing significant memory usage before passing them to the _strvals_ functions.	6.5	More Details
CVE-2022-28199	NVIDIA’s distribution of the Data Plane Development Kit (MLNX_DPDK) contains a vulnerability in the network stack, where error recovery is not handled properly, which can allow a remote attacker to cause denial of service and some impact to data integrity and confidentiality.	6.5	More Details
CVE-2022-38749	Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow.	6.5	More Details
CVE-2022-38750	Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow.	6.5	More Details
CVE-2022-2515	The Simple Banner plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `pro_version_activation_code` parameter in versions up to, and including, 2.11.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, including those without administrative capabilities when access is granted to those users, to inject arbitrary web scripts in page that will execute whenever a user role having access to "Simple Banner" accesses the plugin's settings.	6.4	More Details
CVE-2022-2716	The Beaver Builder – WordPress Page Builder for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Text Editor' block in versions up to, and including, 2.5.5.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with access to the Beaver Builder editor to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2022-2695	The Beaver Builder – WordPress Page Builder for WordPress is vulnerable to Stored Cross-Site Scripting via the 'caption' parameter added to images via the media uploader in versions up to, and including, 2.5.5.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with access to the Beaver Builder editor and the ability to upload media files to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2022-2935	The Image Hover Effects Ultimate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Media Image URL value that can be added to an Image Hover in versions up to, and including, 9.7.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. By default, the plugin only allows administrators access to edit Image Hovers, however, if a site admin makes the plugin's features available to lower privileged users through the 'Who Can Edit?' setting then this can be exploited by those users.	6.4	More Details
CVE-2022-26450	In apusys, 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: ALPS07177801; Issue ID: ALPS07177801.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31152	Synapse is an open-source Matrix homeserver written and maintained by the Matrix.org Foundation. The Matrix specification specifies a list of [event authorization rules](https://spec.matrix.org/v1.2/rooms/v9/#authorization-rules) which must be checked when determining if an event should be accepted into a room. In versions of Synapse up to and including version 1.61.0, some of these rules are not correctly applied. An attacker could craft events which would be accepted by Synapse but not a spec-conformant server, potentially causing divergence in the room state between servers. Administrators of homeservers with federation enabled are advised to upgrade to version 1.62.0 or higher. Federation can be disabled by setting [`federation_domain_whitelist`](https://matrix-org.github.io/synapse/latest/usage/configuration/config_documentation.html#federation_domain_whitelist) to an empty list (`[]`) as a workaround.	6.4	More Details
CVE-2022-2516	The Visual Composer Website Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the post/page 'Title' value in versions up to, and including, 45.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with access to the visual composer editor to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2022-2517	The Beaver Builder – WordPress Page Builder for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Caption - On Hover' value associated with images in versions up to, and including, 2.5.5.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with access to the Beaver Builder editor to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2022-2934	The Beaver Builder – WordPress Page Builder for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Image URL' value found in the Media block in versions up to, and including, 2.5.5.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with access to the Beaver Builder editor to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2022-1628	The Simple SEO plugin for WordPress is vulnerable to attribute-based stored Cross-Site Scripting in versions up to, and including 1.7.91, due to insufficient sanitization or escaping on the SEO social and standard title parameters. This can be exploited by authenticated users with Contributor and above permissions to inject arbitrary web scripts into posts/pages that execute whenever an administrator access the page.	6.4	More Details
CVE-2022-2430	The Visual Composer Website Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Text Block' feature in versions up to, and including, 45.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with access to the visual composer editor to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2022-2936	The Image Hover Effects Ultimate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Video Link values that can be added to an Image Hover in versions up to, and including, 9.7.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. By default, the plugin only allows administrators access to edit Image Hovers, however, if a site admin makes the plugin's features available to lower privileged users through the 'Who Can Edit?' setting then this can be exploited by those users.	6.4	More Details
CVE-2022-29062	Multiple relative path traversal vulnerabilities [CWE-23] in Fortinet FortiSOAR before 7.2.1 allows an authenticated attacker to write to the underlying filesystem with nginx permissions via crafted HTTP requests.	6.3	More Details
CVE-2022-31233	Unisphere for PowerMax versions before 9.2.3.15 contain a privilege escalation vulnerability. An adjacent malicious user may potentially exploit this vulnerability to escalate their privileges and access functionalities they do not have access to.	6.3	More Details
CVE-2021-43076	An improper privilege management vulnerability [CWE-269] in FortiADC versions 6.2.1 and below, 6.1.5 and below, 6.0.4 and below, 5.4.5 and below and 5.3.7 and below may allow a remote authenticated attacker with restricted user profile to modify the system files using the shell access.	6.3	More Details
CVE-2022-35847	An improper neutralization of special elements used in a template engine vulnerability [CWE-1336] in FortiSOAR management interface 7.2.0, 7.0.0 through 7.0.3, 6.4.0 through 6.4.4 may allow a remote and authenticated attacker to execute arbitrary code via a crafted payload.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3122	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file medicine_details.php. The manipulation of the argument medicine leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-207854 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-1677	In OpenShift Container Platform, a user with permissions to create or modify Routes can craft a payload that inserts a malformed entry into one of the cluster router's HAProxy configuration files. This malformed entry can match any arbitrary hostname, or all hostnames in the cluster, and direct traffic to an arbitrary application within the cluster, including one under attacker control.	6.3	More Details
CVE-2022-22101	Denial of service in multimedia due to uncontrolled resource consumption while parsing an incoming HAB message in Snapdragon Auto	6.2	More Details
CVE-2021-35135	A null pointer dereference may potentially occur during RSA key import in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	6.2	More Details
CVE-2022-36583	DedeCMS V5.7.97 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities at /dede/co_do.php via the dopost, rpok, and aid parameters.	6.1	More Details
CVE-2022-2898	Measuresoft ScadaPro Server and Client (All Versions) do not properly resolve links before file access; this could allow a denial-of-service condition.	6.1	More Details
CVE-2022-37183	Piwigo 12.3.0 is vulnerable to Cross Site Scripting (XSS) via /search/1940/created-monthly-list.	6.1	More Details
CVE-2022-2543	The Visual Portfolio, Photo Gallery & Post Grid WordPress plugin before 2.18.0 does not have proper authorisation checks in some of its REST endpoints, allowing unauthenticated users to call them and inject arbitrary CSS in arbitrary saved layouts	6.1	More Details
CVE-2022-38131	RStudio Connect prior to 2023.01.0 is affected by an Open Redirect issue. The vulnerability could allow an attacker to redirect users to malicious websites.	6.1	More Details
CVE-2022-1508	An out-of-bounds read flaw was found in the Linux kernel’s io_uring module in the way a user triggers the io_read() function with some special parameters. This flaw allows a local user to read some memory out of bounds.	6.1	More Details
CVE-2022-39842	An issue was discovered in the Linux kernel before 5.19. In pxa3xx_gcu_write in drivers/video/fbdev/pxa3xx-gcu.c, the count parameter has a type conflict of size_t versus int, causing an integer overflow and bypassing the size check. After that, because it is used as the third argument to copy_from_user(), a heap overflow may occur. NOTE: the original discoverer disputes that the overflow can actually happen.	6.1	More Details
CVE-2022-3123	Cross-site Scripting (XSS) - Reflected in GitHub repository splitbrain/dokuwiki prior to 2022-07-31a.	6.1	More Details
CVE-2022-36203	Doctor's Appointment System 1.0 is vulnerable to Cross Site Scripting (XSS) via the admin panel. In addition, it leads to takeover the administrator account by stealing the cookie via XSS.	6.1	More Details
CVE-2022-26331	Potential vulnerabilities have been identified in Micro Focus ArcSight Logger. The vulnerabilities could be remotely exploited resulting in Information Disclosure, or Self Cross-Site Scripting (XSS). This issue affects: Micro Focus ArcSight Logger versions prior to v7.2.2 version and prior versions.	6.1	More Details
CVE-2022-1355	A stack buffer overflow flaw was found in Libtiffs' tiffcp.c in main() function. This flaw allows an attacker to pass a crafted TIFF file to the tiffcp tool, triggering a stack buffer overflow issue, possibly corrupting the memory, and causing a crash that leads to a denial of service.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35933	This package is a PrestaShop module that allows users to post reviews and rate products. There is a vulnerability where the attacker could steal an administrator's cookie. The issue is fixed in version 5.0.2.	6.1	More Details
CVE-2022-26858	Dell BIOS versions contain an Improper Authentication vulnerability. A locally authenticated malicious user could potentially exploit this vulnerability by sending malicious input to an SMI in order to bypass security controls.	6.1	More Details
CVE-2022-36796	Cross-Site Request Forgery (CSRF) vulnerability leading to Stored Cross-Site Scripting (XSS) in CallRail, Inc. CallRail Phone Call Tracking plugin <= 0.4.9 at WordPress.	6.1	More Details
CVE-2022-26859	Dell BIOS contains a race condition vulnerability. A local attacker could exploit this vulnerability by sending malicious input via SMI in order to bypass security checks during SMM.	6.1	More Details
CVE-2022-36064	Shescape is a shell escape package for JavaScript. An Inefficient Regular Expression Complexity vulnerability impacts users that use Shescape to escape arguments for the Unix shells `Bash` and `Dash`, or any not-officially-supported Unix shell; and/or using the `escape` or `escapeAll` functions with the `interpolation` option set to `true`. An attacker can cause polynomial backtracking or quadratic runtime in terms of the input string length due to two Regular Expressions in Shescape that are vulnerable to Regular Expression Denial of Service (ReDoS). This bug has been patched in v1.5.10. For `Dash` only, this bug has been patched since v1.5.9. As a workaround, a maximum length can be enforced on input strings to Shescape to reduce the impact of the vulnerability. It is not recommended to try and detect vulnerable input strings, as the logic for this may end up being vulnerable to ReDoS itself.	5.9	More Details
CVE-2022-36072	SilverwareGames.io is a social network for users to play video games online. In version 1.1.8 and prior, due to an unobvious feature of PHP, hashes generated by built-in functions and starting with the `0e` symbols were being handled as zero multiplied with the `e` number. Therefore, the hash value was equal to 0. The maintainers fixed this in version 1.1.9 by using `===` instead of `==` in comparisons where it is possible (e.g. on sign in/sign up handlers).	5.9	More Details
CVE-2021-44718	wolfSSL through 5.0.0 allows an attacker to cause a denial of service and infinite loop in the client component by sending crafted traffic from a Machine-in-the-Middle (MITM) position. The root cause is that the client module accepts TLS messages that normally are only sent to TLS servers.	5.9	More Details
CVE-2022-23678	A vulnerability in the Aruba Virtual Intranet Access (VIA) client for Microsoft Windows operating system client communications that could allow for an attacker in a privileged network position to intercept sensitive information in Aruba Virtual Intranet Access (VIA) client for Microsoft Windows operating system versions: 4.3.0 build 2208101 and below. Aruba has released upgrades for Virtual Intranet Access (VIA) Client that address this security vulnerability.	5.9	More Details
CVE-2022-36052	Contiki-NG is an open-source, cross-platform operating system for Next-Generation IoT devices. The 6LoWPAN implementation in Contiki-NG may cast a UDP header structure at a certain offset in a packet buffer. The code does not check whether the packet buffer is large enough to fit a full UDP header structure from the offset where the casting is made. Hence, it is possible to cause an out-of-bounds read beyond the packet buffer. The problem affects anyone running devices with Contiki-NG versions previous to 4.8, and which may receive 6LoWPAN packets from external parties. The problem has been patched in Contiki-NG version 4.8.	5.9	More Details
CVE-2022-36053	Contiki-NG is an open-source, cross-platform operating system for Next-Generation IoT devices. The low-power IPv6 network stack of Contiki-NG has a buffer module (os/net/ipv6/uipbuf.c) that processes IPv6 extension headers in incoming data packets. As part of this processing, the function uipbuf_get_next_header casts a pointer to a uip_ext_hdr structure into the packet buffer at different offsets where extension headers are expected to be found, and then reads from this structure. Because of a lack of bounds checking, the casting can be done so that the structure extends beyond the packet's end. Hence, with a carefully crafted packet, it is possible to cause the Contiki-NG system to read data outside the packet buffer. A patch that fixes the vulnerability is included in Contiki-NG 4.8.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38153	An issue was discovered in wolfSSL before 5.5.0 (when --enable-session-ticket is used); however, only version 5.3.0 is exploitable. Man-in-the-middle attackers or a malicious server can crash TLS 1.2 clients during a handshake. If an attacker injects a large ticket (more than 256 bytes) into a NewSessionTicket message in a TLS 1.2 handshake, and the client has a non-empty session cache, the session cache frees a pointer that points to unallocated memory, causing the client to crash with a "free(): invalid pointer" message. NOTE: It is likely that this is also exploitable during TLS 1.3 handshakes between a client and a malicious server. With TLS 1.3, it is not possible to exploit this as a man-in-the-middle.	5.9	More Details
CVE-2022-1263	A NULL pointer dereference issue was found in KVM when releasing a vCPU with dirty ring support enabled. This flaw allows an unprivileged local attacker on the host to issue specific ioctl calls, causing a kernel oops condition that results in a denial of service.	5.5	More Details
CVE-2022-1325	A flaw was found in Clmg, where with the help of a maliciously crafted pandore or bmp file with modified dx and dy header field values it is possible to trick the application into allocating huge buffer sizes like 64 Gigabyte upon reading the file from disk or from a virtual buffer.	5.5	More Details
CVE-2022-28625	A local disclosure of sensitive information vulnerability was discovered in HPE OneView version(s): Prior to 7.0 or 6.60.01. A low privileged user could locally exploit this vulnerability to disclose sensitive information resulting in a complete loss of confidentiality, integrity, and availability. To exploit this vulnerability, HPE OneView must be configured with credential access to external repositories. HPE has provided a software update to resolve this vulnerability in HPE OneView.	5.5	More Details
CVE-2022-1354	A heap buffer overflow flaw was found in Libtiffs' tiffinfo.c in TIFFReadRawDataStriped() function. This flaw allows an attacker to pass a crafted TIFF file to the tiffinfo tool, triggering a heap buffer overflow issue and causing a crash that leads to a denial of service.	5.5	More Details
CVE-2022-2473	The WP-UserOnline plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘templates[browsingpage][text]' parameter in versions up to, and including, 2.87.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with administrative capabilities and above to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The only affects multi-site installations and installations where unfiltered_html is disabled.	5.5	More Details
CVE-2020-35538	A crafted input file could cause a null pointer dereference in jcopy_sample_rows() when processed by libjpeg-turbo.	5.5	More Details
CVE-2022-1975	There is a sleep-in-atomic bug in /net/nfc/netlink.c that allows an attacker to crash the Linux kernel by simulating a nfc device from user-space.	5.5	More Details
CVE-2022-2941	The WP-UserOnline plugin for WordPress has multiple Stored Cross-Site Scripting vulnerabilities in versions up to, and including 2.88.0. This is due to the fact that all fields in the "Naming Conventions" section do not properly sanitize user input, nor escape it on output. This makes it possible for authenticated attackers, with administrative privileges, to inject JavaScript code into the setting that will execute whenever a user accesses the injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	5.5	More Details
CVE-2020-27784	A vulnerability was found in the Linux kernel, where accessing a deallocated instance in printer_ioctl() printer_ioctl() tries to access of a printer_dev instance. However, use-after-free arises because it had been freed by gprinter_free().	5.5	More Details
CVE-2022-36647	PKUVCL davs2 v1.6.205 was discovered to contain a global buffer overflow via the function parse_sequence_header() at source/common/header.cc:269.	5.5	More Details
CVE-2022-2153	A flaw was found in the Linux kernel’s KVM when attempting to set a SynIC IRQ. This issue makes it possible for a misbehaving VMM to write to SYNIC/STIMER MSRs, causing a NULL pointer dereference. This flaw allows an unprivileged local attacker on the host to issue specific ioctl calls, causing a kernel oops condition that results in a denial of service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25310	A segmentation fault (SEGV) flaw was found in the Fribidi package and affects the fribidi_remove_bidi_marks() function of the lib/fribidi.c file. This flaw allows an attacker to pass a specially crafted file to Fribidi, leading to a crash and causing a denial of service.	5.5	More Details
CVE-2022-34378	Dell PowerScale OneFS, versions 9.0.0 up to and including 9.1.0.20, 9.2.1.13, 9.3.0.6, and 9.4.0.3, contain a relative path traversal vulnerability. A low privileged local attacker could potentially exploit this vulnerability, leading to denial of service.	5.5	More Details
CVE-2022-2759	Delta Electronics Delta Robot Automation Studio (DRAS) versions prior to 1.13.20 are affected by improper restrictions where the software processes an XML document that can contain XML entities with URIs that resolve to documents outside of the intended sphere of control, causing the product to embed incorrect documents into its output. This may allow an attacker to view sensitive documents and information on the affected host.	5.5	More Details
CVE-2022-1615	In Samba, GnuTLS gnutls_rnd() can fail and give predictable random values.	5.5	More Details
CVE-2021-39045	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.2.1 could allow a local attacker to obtain information due to the autocomplete feature on password input fields. IBM X-Force ID: 214345.	5.5	More Details
CVE-2021-39009	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.2.1 stores user credentials in plain clear text which can be read by a local privileged user. IBM X-Force ID: 213554.	5.5	More Details
CVE-2022-2775	The Fast Flow WordPress plugin before 1.2.13 does not sanitise and escape some of its Widget 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)	5.5	More Details
CVE-2020-35535	In LibRaw, there is an out-of-bounds read vulnerability within the "LibRaw::parseSonySRF()" function (libraw\src\metadata\sony.cpp) when processing srf files.	5.5	More Details
CVE-2022-3061	Found Linux Kernel flaw in the i740 driver. The Userspace program could pass any values to the driver through ioctl() interface. The driver doesn't check the value of 'pixclock', so it may cause a divide by zero error.	5.5	More Details
CVE-2020-35534	In LibRaw, there is a memory corruption vulnerability within the "crxFreeSubbandData()" function (libraw\src\decoders\crx.cpp) when processing cr3 files.	5.5	More Details
CVE-2020-35533	In LibRaw, an out-of-bounds read vulnerability exists within the "LibRaw::adobe_copy_pixel()" function (libraw\src\decoders\dng.cpp) when reading data from the image file.	5.5	More Details
CVE-2020-35532	In LibRaw, an out-of-bounds read vulnerability exists within the "simple_decode_row()" function (libraw\src\x3f\x3f_utils_patched.cpp) which can be triggered via an image with a large row_stride field.	5.5	More Details
CVE-2022-3078	An issue was discovered in the Linux kernel through 5.16-rc6. There is a lack of check after calling vzalloc() and lack of free after allocation in drivers/media/test-drivers/vidtv/vidtv_s302m.c.	5.5	More Details
CVE-2020-35531	In LibRaw, an out-of-bounds read vulnerability exists within the get_huffman_diff() function (libraw\src\x3f\x3f_utils_patched.cpp) when reading data from an image file.	5.5	More Details
CVE-2022-2806	It was found that the ovirt-log-collector/sosreport collects the RHV admin password unfiltered. Fixed in: sos-4.2-20.el8_6, ovirt-log-collector-4.4.7-2.el8ev	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25309	A heap-based buffer overflow flaw was found in the Fribidi package and affects the fribidi_cap_rtl_to_unicode() function of the fribidi-char-sets-cap-rtl.c file. This flaw allows an attacker to pass a specially crafted file to the Fribidi application with the '--caprtl' option, leading to a crash and causing a denial of service.	5.5	More Details
CVE-2020-35530	In LibRaw, there is an out-of-bounds write vulnerability within the "new_node()" function (libraw\src\x3f\x3f_utils_patched.cpp) that can be triggered via a crafted X3F file.	5.5	More Details
CVE-2022-39190	An issue was discovered in net/netfilter/nf_tables_api.c in the Linux kernel before 5.19.6. A denial of service can occur upon binding to an already bound chain.	5.5	More Details
CVE-2022-36639	A stored cross-site scripting (XSS) vulnerability in /client.php of Garage Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the name parameter.	5.4	More Details
CVE-2022-38790	Weave GitOps Enterprise before 0.9.0-rc.5 has a cross-site scripting (XSS) bug allowing a malicious user to inject a javascript: link in the UI. When clicked by a victim user, the script will execute with the victim's permission. The exposure appears in Weave GitOps Enterprise UI via a GitopsCluster dashboard link. An annotation can be added to a GitopsCluster custom resource.	5.4	More Details
CVE-2022-31792	A stored cross-site scripting (XSS) vulnerability exists in the management web interface of WatchGuard Firebox and XTM appliances. A remote attacker can potentially execute arbitrary JavaScript code in the management web interface by sending crafted requests to exposed management ports. This is fixed in Fireware OS 12.8.1, 12.5.10, and 12.1.4.	5.4	More Details
CVE-2022-2597	The Visual Portfolio, Photo Gallery & Post Grid WordPress plugin before 2.19.0 does not have proper authorisation checks in some of its REST endpoints, allowing users with a role as low as contributor to call them and inject arbitrary CSS in arbitrary saved layouts	5.4	More Details
CVE-2022-25370	Apache OFBiz uses the Birt plugin (https://eclipse.github.io/birt-website/) to create data visualizations and reports. In Apache OFBiz release 18.12.05, and earlier versions, by leveraging a vulnerability in Birt (https://bugs.eclipse.org/bugs/show_bug.cgi?id=538142), an unauthenticated malicious user could perform a stored XSS attack in order to inject a malicious payload and execute it using the stored XSS.	5.4	More Details
CVE-2022-36355	Authenticated (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in PluginlySpeaking Easy Org Chart plugin <= 3.1 at WordPress.	5.4	More Details
CVE-2022-36057	Discourse-Chat is an asynchronous messaging plugin for the Discourse open-source discussion platform. Users of Discourse Chat can be affected by admin users inserting HTML into chat titles and descriptions, causing a Cross-Site Scripting (XSS) attack. Version 0.9 contains a patch for this issue.	5.4	More Details
CVE-2022-3127	Cross-site Scripting (XSS) - Stored in GitHub repository jgraph/drawio prior to 20.2.8.	5.4	More Details
CVE-2022-26114	An improper neutralization of input during web page generation vulnerability [CWE-79] in the Webmail of FortiMail before 7.2.0 may allow an unauthenticated attacker to trigger a cross-site scripting (XSS) attack via sending specially crafted mail messages.	5.4	More Details
CVE-2022-36637	Garage Management System v1.0 was discovered to contain a persistent cross-site scripting (XSS) vulnerability via the brand_name parameter at /brand.php.	5.4	More Details
CVE-2022-33177	Cross-Site Request Forgery (CSRF) vulnerability in WPdevelop/Oplugins Booking Calendar plugin <= 9.2.1 at WordPress leading to Translations Update.	5.4	More Details
CVE-2022-3072	Cross-site Scripting (XSS) - Stored in GitHub repository francoisjacquet/rosariosis prior to 8.9.3.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36373	Multiple Cross-Site Request Forgery (CSRF) vulnerabilities in Simon Ward MP3 jPlayer plugin <= 2.7.3 at WordPress.	5.4	More Details
CVE-2022-37253	Persistent cross-site scripting (XSS) in Crime Reporting System 1.0 allows a remote attacker to introduce arbitary Javascript via manipulation of an unsanitized POST parameter	5.4	More Details
CVE-2022-36425	Broken Access Control vulnerability in Beaver Builder plugin <= 2.5.4.3 at WordPress.	5.4	More Details
CVE-2022-2739	The version of podman as released for Red Hat Enterprise Linux 7 Extras via RHSA-2022:2190 advisory included an incorrect version of podman missing the fix for CVE-2020-14370, which was previously fixed via RHSA-2020:5056. This issue could possibly allow an attacker to gain access to sensitive information stored in environment variables.	5.3	More Details
CVE-2022-2663	An issue was found in the Linux kernel in nf_conntrack_irc where the message handling can be confused and incorrectly matches the message. A firewall may be able to be bypassed when users are using unencrypted IRC with nf_conntrack_irc configured.	5.3	More Details
CVE-2022-36046	Next.js is a React framework that can provide building blocks to create web applications. All of the following must be true to be affected by this CVE: Next.js version 12.2.3, Node.js version above v15.0.0 being used with strict `unhandledRejection` exiting AND using next start or a [custom server](https://nextjs.org/docs/advanced-features/custom-server). Deployments on Vercel (vercel.com) are not affected along with similar environments where `next-server` isn't being shared across requests.	5.3	More Details
CVE-2022-36638	An access control issue in the component print.php of Garage Management System v1.0 allows unauthenticated attackers to access data for all existing orders.	5.3	More Details
CVE-2022-2939	The WP Cerber Security plugin for WordPress is vulnerable to security protection bypass in versions up to, and including 9.0, that makes user enumeration possible. This is due to improper validation on the value supplied through the 'author' parameter found in the ~/cerber-load.php file. In vulnerable versions, the plugin only blocks requests if the value supplied is numeric, making it possible for attackers to supply additional non-numeric characters to bypass the protection. The non-numeric characters are stripped and the user requested is displayed. This can be used by unauthenticated attackers to gather information about users that can targeted in further attacks.	5.3	More Details
CVE-2022-2462	The Transposh WordPress Translation plugin for WordPress is vulnerable to sensitive information disclosure to unauthenticated users in versions up to, and including, 1.0.8.1. This is due to insufficient permissions checking on the 'tp_history' AJAX action and insufficient restriction on the data returned in the response. This makes it possible for unauthenticated users to exfiltrate usernames of individuals who have translated text.	5.3	More Details
CVE-2022-36032	ReactPHP HTTP is a streaming HTTP client and server implementation for ReactPHP. In ReactPHP's HTTP server component versions starting with 0.7.0 and prior to 1.7.0, when ReactPHP is processing incoming HTTP cookie values, the cookie names are url-decoded. This may lead to cookies with prefixes like `__Host-` and `__Secure-` confused with cookies that decode to such prefix, thus leading to an attacker being able to forge cookie which is supposed to be secure. This issue is fixed in ReactPHP HTTP version 1.7.0. As a workaround, Infrastructure or DevOps can place a reverse proxy in front of the ReactPHP HTTP server to filter out any unexpected `Cookie` request headers.	5.3	More Details
CVE-2022-23690	A vulnerability in the web-based management interface of AOS-CX could allow a remote unauthenticated attacker to fingerprint the exact version AOS-CX running on the switch. This allows an attacker to retrieve information which could be used to more precisely target the switch for further exploitation in ArubaOS-CX Switches version(s): AOS-CX 10.10.xxxx: 10.10.0002 and below, AOS-CX 10.09.xxxx: 10.09.1020 and below, AOS-CX 10.08.xxxx: 10.08.1060 and below, AOS-CX 10.06.xxxx: 10.06.0200 and below. Aruba has released upgrades for ArubaOS-CX Switch Devices that address this security vulnerability.	5.3	More Details
CVE-2022-1522	The Cognex 3D-A1000 Dimensioning System in firmware version 1.0.3 (3354) and prior is vulnerable to CWE-117: Improper Output Neutralization for Logs, which allows an attacker to create false logs that show the password as having been changed when it is not, complicating forensics.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2461	The Transposh WordPress Translation plugin for WordPress is vulnerable to unauthorized setting changes by unauthenticated users in versions up to, and including, 1.0.8.1. This is due to insufficient permissions checking on the 'tp_translation' AJAX action and default settings which makes it possible for unauthenticated attackers to influence the data shown on the site.	5.3	More Details
CVE-2022-2376	The Directorist WordPress plugin before 7.3.1 discloses the email address of all users in an AJAX action available to both unauthenticated and any authenticated users	5.3	More Details
CVE-2022-32277	Squiz Matrix CMS 6.20 is vulnerable to an Insecure Direct Object Reference caused by failure to correctly validate authorization when submitting a request to change a user's contact details. NOTE: this is disputed by both the vendor and the original discoverer because it is a site-specific finding, not a finding about the Squiz Matrix CMS product.	5.3	More Details
CVE-2022-27911	An issue was discovered in Joomla! 4.2.0. Multiple Full Path Disclosures because of missing '_JEXEC or die check' caused by the PSR12 changes.	5.3	More Details
CVE-2022-38367	The Netic User Export add-on before 2.0.6 for Atlassian Jira does not perform authorization checks. This might allow an unauthenticated user to export all users from Jira by making an HTTP request to the affected endpoint.	5.3	More Details
CVE-2022-2945	The WordPress Infinite Scroll – Ajax Load More plugin for WordPress is vulnerable to Directory Traversal in versions up to, and including, 5.5.3 via the 'type' parameter found in the alm_get_layout() function. This makes it possible for authenticated attackers, with administrative permissions, to read the contents of arbitrary files on the server, which can contain sensitive information.	4.9	More Details
CVE-2022-2764	A flaw was found in Undertow. Denial of service can be achieved as Undertow server waits for the LAST_CHUNK forever for EJB invocations.	4.9	More Details
CVE-2022-23452	An authorization flaw was found in openstack-barbican, where anyone with an admin role could add secrets to a different project container. This flaw allows an attacker on the network to consume protected resources and cause a denial of service.	4.9	More Details
CVE-2022-2943	The WordPress Infinite Scroll – Ajax Load More plugin for Wordpress is vulnerable to arbitrary file reading in versions up to, and including, 5.5.3 due to insufficient file path validation on the alm_repeaters_export() function. This makes it possible for authenticated attackers, with administrative privileges, to download arbitrary files hosted on the server that may contain sensitive content, such as the wp-config.php file.	4.9	More Details
CVE-2022-39194	An issue was discovered in the MediaWiki through 1.38.2. The community configuration pages for the GrowthExperiments extension could cause a site to become unavailable due to insufficient validation when certain actions (including page moves) were performed.	4.9	More Details
CVE-2022-39840	Cotonti Siena 0.9.20 allows admins to conduct stored XSS attacks via a direct message (DM).	4.8	More Details
CVE-2022-37679	Miniblog.Core v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the component /blog/edit. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Excerpt field.	4.8	More Details
CVE-2022-36600	BlogEngine v3.3.8.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the component /blogengine/api/posts. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Description field.	4.8	More Details
CVE-2021-36829	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability in MyThemeShop Launcher: Coming Soon & Maintenance Mode plugin <= 1.0.11 at WordPress.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34656	Authenticated (admin+) Cross-Site Scripting (XSS) vulnerability in wpdevart Poll, Survey, Questionnaire and Voting system plugin <= 1.7.4 at WordPress.	4.8	More Details
CVE-2022-2271	The WP Database Backup WordPress plugin before 5.9 does not escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-39839	Cotonti Siena 0.9.20 allows admins to conduct stored XSS attacks via a forum post.	4.8	More Details
CVE-2022-39188	An issue was discovered in include/asm-generic/tlb.h in the Linux kernel before 5.19. Because of a race condition (unmap_mapping_range versus munmap), a device driver can free a page while it still has stale TLB entries. This only occurs in situations with VM_PFNMAP VMAs.	4.7	More Details
CVE-2022-1205	A NULL pointer dereference flaw was found in the Linux kernel's Amateur Radio AX.25 protocol functionality in the way a user connects with the protocol. This flaw allows a local user to crash the system.	4.7	More Details
CVE-2022-38170	In Apache Airflow prior to 2.3.4, an insecure umask was configured for numerous Airflow components when running with the `--daemon` flag which could result in a race condition giving world-writable files in the Airflow home directory and allowing local users to expose arbitrary file contents via the webserver.	4.7	More Details
CVE-2021-43080	An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiOS version 7.2.0, version 6.4.0 through 6.4.9, version 7.0.0 through 7.0.5 may allow an authenticated attacker to perform a stored cross site scripting (XSS) attack through the URI parameter via the Threat Feed IP address section of the Security Fabric External connectors.	4.6	More Details
CVE-2022-39050	An attacker who is logged into OTRS as an admin user may manipulate customer URL field to store JavaScript code to be run later by any other agent when clicking the customer URL link. Then the stored JavaScript is executed in the context of OTRS. The same issue applies for the usage of external data sources e.g. database or ldap	4.6	More Details
CVE-2022-26456	In vow, there is a possible information disclosure due to a symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06545473; Issue ID: ALPS06545473.	4.4	More Details
CVE-2022-26463	In vow, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032686; Issue ID: ALPS07032686.	4.4	More Details
CVE-2022-26459	In vow, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032634; Issue ID: ALPS07032634.	4.4	More Details
CVE-2022-26462	In vow, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032660; Issue ID: ALPS07032660.	4.4	More Details
CVE-2022-3121	A vulnerability was found in SourceCodester Online Employee Leave Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/addemployee.php. The manipulation leads to cross-site request forgery. The attack can be launched remotely. The identifier VDB-207853 was assigned to this vulnerability.	4.3	More Details
CVE-2022-35913	Samourai Wallet Stonewallx2 0.99.98e allows a denial of service via a P2P coinjoin. The attacker and victim must follow each other's paynym. Then, the victim must try to collaborate with the attacker for a Stonewallx2 transaction. Next, the attacker broadcasts a tx, spending the inputs used in Stonewallx2 before the victim can broadcast the collaborative transaction. The attacker does not signal opt in RBF, and uses the lowest fee rate. This would result in the victim being unable to perform Stonewallx2. (Note that the attacker could use multiple paynyms.)	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23687	Multiple vulnerabilities exist in the processing of packet data by the LLDP service of AOS-CX. Successful exploitation of these vulnerabilities may allow an attacker to impact the availability of the AOS-CX LLDP service and/or the management plane of the switch in ArubaOS-CX Switches version(s): AOS-CX 10.09.xxxx: 10.09.1010 and below, AOS-CX 10.08.xxxx: 10.08.1050 and below, AOS-CX 10.06.xxxx: 10.06.0190 and below. Aruba has released upgrades for ArubaOS-CX Switch Devices that address these security vulnerabilities.	4.3	More Details
CVE-2022-23688	Multiple vulnerabilities exist in the processing of packet data by the LLDP service of AOS-CX. Successful exploitation of these vulnerabilities may allow an attacker to impact the availability of the AOS-CX LLDP service and/or the management plane of the switch in ArubaOS-CX Switches version(s): AOS-CX 10.09.xxxx: 10.09.1010 and below, AOS-CX 10.08.xxxx: 10.08.1050 and below, AOS-CX 10.06.xxxx: 10.06.0190 and below. Aruba has released upgrades for ArubaOS-CX Switch Devices that address these security vulnerabilities.	4.3	More Details
CVE-2022-28884	A Denial-of-Service vulnerability was discovered in the F-Secure and WithSecure products where aerdl.dll may go into an infinite loop when unpacking PE files. It is possible that this can crash the scanning engine.	4.3	More Details
CVE-2022-36048	Zulip is an open-source team collaboration tool with topic-based threading that combines email and chat. When displaying messages with embedded remote images, Zulip normally loads the image preview via a go-camo proxy server. However, an attacker who can send messages could include a crafted URL that tricks the server into embedding a remote image reference directly. This could allow the attacker to infer the viewer's IP address and browser fingerprinting information. This vulnerability is fixed in Zulip Server 5.6. Zulip organizations with image and link previews [disabled](https://zulip.com/help/allow-image-link-previews) are not affected.	4.3	More Details
CVE-2022-23689	Multiple vulnerabilities exist in the processing of packet data by the LLDP service of AOS-CX. Successful exploitation of these vulnerabilities may allow an attacker to impact the availability of the AOS-CX LLDP service and/or the management plane of the switch in ArubaOS-CX Switches version(s): AOS-CX 10.09.xxxx: 10.09.1010 and below, AOS-CX 10.08.xxxx: 10.08.1050 and below, AOS-CX 10.06.xxxx: 10.06.0190 and below. Aruba has released upgrades for ArubaOS-CX Switch Devices that address these security vulnerabilities.	4.3	More Details
CVE-2022-28885	A Denial-of-Service (DoS) vulnerability was discovered in the fsicapd component used in WithSecure products whereby the service may crash while parsing the scanning request.	4.3	More Details
CVE-2022-2657	The Multivendor Marketplace Solution for WooCommerce WordPress plugin before 3.8.12 is lacking authorisation and CSRF in multiple AJAX actions, which could allow any authenticated users, such as subscriber to call them and suspend vendors (reporter by the submitter) or update arbitrary order status (identified by WPScan when verifying the issue) for example. Other unauthenticated attacks are also possible, either directly or via CSRF	4.3	More Details
CVE-2022-23686	Multiple vulnerabilities exist in the processing of packet data by the LLDP service of AOS-CX. Successful exploitation of these vulnerabilities may allow an attacker to impact the availability of the AOS-CX LLDP service and/or the management plane of the switch in ArubaOS-CX Switches version(s): AOS-CX 10.09.xxxx: 10.09.1010 and below, AOS-CX 10.08.xxxx: 10.08.1050 and below, AOS-CX 10.06.xxxx: 10.06.0190 and below. Aruba has released upgrades for ArubaOS-CX Switch Devices that address these security vulnerabilities.	4.3	More Details
CVE-2022-1974	A use-after-free flaw was found in the Linux kernel's NFC core functionality due to a race condition between kobject creation and delete. This vulnerability allows a local attacker with CAP_NET_ADMIN privilege to leak kernel information.	4.1	More Details
CVE-2022-1697	Okta Active Directory Agent versions 3.8.0 through 3.11.0 installed the Okta AD Agent Update Service using an unquoted path. Note: To remediate this vulnerability, you must uninstall Okta Active Directory Agent and reinstall Okta Active Directory Agent 3.12.0 or greater per the documentation.	3.9	More Details
CVE-2022-2256	A Stored Cross-site scripting (XSS) vulnerability was found in keycloak as shipped in Red Hat Single Sign-On 7. This flaw allows a privileged attacker to execute malicious scripts in the admin console, abusing the default roles functionality.	3.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39049	An attacker who is logged into OTRS as an admin user may manipulate the URL to cause execution of JavaScript in the context of OTRS.	3.5	More Details
CVE-2022-1404	Delta Electronics CNCSoft (All versions prior to 1.01.32) does not properly sanitize input while processing a specific project file, allowing a possible out-of-bounds read condition.	3.3	More Details
CVE-2022-35931	Nextcloud Password Policy is an app that enables a Nextcloud server admin to define certain rules for passwords. Prior to versions 22.2.10, 23.0.7, and 24.0.3 the random password generator may, in very rare cases, generate common passwords that the validator itself would block. Upgrade Nextcloud Server to 22.2.10, 23.0.7 or 24.0.3 to receive a patch for the issue in Password Policy. There are no known workarounds available.	2.7	More Details
CVE-2022-29053	A missing cryptographic steps vulnerability [CWE-325] in the functions that encrypt the keytab files in FortiOS version 7.2.0, 7.0.0 through 7.0.5 and below 7.0.0 may allow an attacker in possession of the encrypted file to decipher it.	2.3	More Details
CVE-2020-35529	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-35528	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-35526	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2022-38126	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-2220	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-1260	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2022-0844	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2022-38127	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-36757	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-2021-39326	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-2021-39324	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-2020-35537	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8586	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2022-38128	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-38289	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-2020-35536	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