SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 05 July 2023

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-22814	An authentication bypass issue via spoofing was discovered in the token-based authentication mechanism that could allow an attacker to carry out an impersonation attack. This issue affects My Cloud OS 5 devices: before 5.26.202.	10.0	More Details
CVE-2023-33190	Sealos is an open source cloud operating system distribution based on the Kubernetes kernel. In versions of Sealos prior to 4.2.1-rc4 an improper configuration of role based access control (RBAC) permissions resulted in an attacker being able to obtain cluster control permissions, which could control the entire cluster deployed with Sealos, as well as hundreds of pods and other resources within the cluster. This issue has been addressed in version 4.2.1-rc4. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36468	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. When an XWiki installation is upgraded and that upgrade contains a fix for a bug in a document, just a new version of that document is added. In some cases, it's still possible to exploit the vulnerability that was fixed in the new version. The severity of this depends on the fixed vulnerability, for the purpose of this advisory take CVE-2022-36100/GHSA-2g5c-228j-p52x as example - it is easily exploitable with just view rights and critical. When XWiki is upgraded from a version before the fix for it (e.g., 14.3) to a version including the fix (e.g., 14.4), the vulnerability can still be reproduced by adding `rev=1.1` to the URL used in the reproduction steps so remote code execution is possible even after upgrading. Therefore, this affects the confidentiality, integrity and availability of the whole XWiki installation. This vulnerability also affects manually added script macros that contained security vulnerabilities that were later fixed by changing the script macro without deleting the versions with the security vulnerability from the history. This vulnerability doesn't affect freshly installed versions of XWiki. Further, this vulnerability doesn't affect content that is only loaded from the current version of a document like the code of wiki macros or UI extensions. This vulnerability has been patched in XWiki 14.10.7 and 15.2RC1 by forcing old revisions to be executed in a restricted mode that disables all script macros. As a workaround, admins can manually delete old revisions of affected documents. A script could be used to identify all installed documents and delete the history for them. However, also manually added and later corrected code may be affected by this vulnerability so it is easy to miss documents.	9.9	More Details
CVE-2023-36469	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user who can edit their own user profile and notification settings can execute arbitrary script macros including Groovy and Python macros that allow remote code execution including unrestricted read and write access to all wiki contents. This has been patched in XWiki 14.10.6 and 15.2RC1. Users are advised to update. As a workaround the main security fix can be manually applied by patching the affected document `XWiki.Notifications.Code.NotificationRSSService`. This will break the link to the differences, though as this requires additional changes to Velocity templates as shown in the patch. While the default template is available in the instance and can be easily patched, the template for mentions is contained in a `.jar`-file and thus cannot be fixed without replacing that jar.	9.9	More Details
CVE-2023-36470	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. By either creating a new or editing an existing document with an icon set, an attacker can inject XWiki syntax and Velocity code that is executed with programming rights and thus allows remote code execution. There are different attack vectors, the simplest is the Velocity code in the icon set's HTML or XWiki syntax definition. The [icon picker](https://extensions.xwiki.org/xwiki/bin/view/Extension/Icon%20Theme%20Application#HIconPicker) can be used to trigger the rendering of any icon set. The XWiki syntax variant of the icon set is also used without any escaping in some documents, allowing to inject XWiki syntax including script macros into a document that might have programming right, for this the currently used icon theme needs to be edited. Further, the HTML output of the icon set is output as JSON in the icon picker and this JSON is interpreted as XWiki syntax, allowing again the injection of script macros into a document with programming right and thus allowing remote code execution. This impacts the confidentiality, integrity and availability of the whole XWiki instance. This issue has been patched in XWiki 14.10.6 and 15.1. Icon themes now require script right and the code in the icon theme is executed within the context of the icon theme, preventing any rights escalation. A macro for displaying icons has been introduced to avoid injecting the raw wiki syntax of an icon set into another document. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.9	More Details
CVE-2023-3490	SQL Injection in GitHub repository fossbilling/fossbilling prior to 0.5.3.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-18432	File Upload vulnerability in SEMCMS PHP 3.7 allows remote attackers to upload arbitrary files and gain escalated privileges.	9.8	More Details
CVE-2023-2834	The BookIt plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 2.3.7. This is due to insufficient verification on the user being supplied during booking an appointment through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email.	9.8	More Details
CVE-2023-3249	The Web3 – Crypto wallet Login & NFT token gating plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 2.6.0. This is due to incorrect authentication checking in the 'hidden_form_data' function. This makes it possible for authenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the username.	9.8	More Details
CVE-2023-35175	Certain HP LaserJet Pro print products are potentially vulnerable to Potential Remote Code Execution and/or Elevation of Privilege via Server-Side Request Forgery (SSRF) using the Web Service Eventing model.	9.8	More Details
CVE-2023-37303	An issue was discovered in the CheckUser extension for MediaWiki through 1.39.3. In certain situations, an attempt to block a user fails after a temporary browser hang and a DBQueryDisconnectedError error message.	9.8	More Details
CVE-2023-31543	A dependency confusion in pipreqs v0.3.0 to v0.4.11 allows attackers to execute arbitrary code via uploading a crafted PyPI package to the chosen repository server.	9.8	More Details
CVE-2023-26134	Versions of the package git-commit-info before 2.0.2 are vulnerable to Command Injection such that the package-exported method gitCommitInfo () fails to sanitize its parameter commit, which later flows into a sensitive command execution API. As a result, attackers may inject malicious commands once they control the hash content.	9.8	More Details
CVE-2023-36487	The password reset function in ILIAS 7.0_beta1 through 7.20 and 8.0_beta1 through 8.1 allows remote attackers to take over the account.	9.8	More Details
CVE-2023-28323	A deserialization of untrusted data exists in EPM 2022 Su3 and all prior versions that allows an unauthenticated user to elevate rights. This exploit could potentially be used in conjunction with other OS (Operating System) vulnerabilities to escalate privileges on the machine or be used as a stepping stone to get to other network attached machines.	9.8	More Details
CVE-2023-28324	A improper input validation vulnerability exists in Ivanti Endpoint Manager 2022 and below that could allow privilege escalation or remote code execution.	9.8	More Details
CVE-2023-35797	Improper Input Validation vulnerability in Apache Software Foundation Apache Airflow Hive Provider. This issue affects Apache Airflow Apache Hive Provider: before 6.1.1. Before version 6.1.1 it was possible to bypass the security check to RCE via principal parameter. For this to be exploited it requires access to modifying the connection details. It is recommended updating provider version to 6.1.1 in order to avoid this vulnerability.	9.8	More Details
CVE-2023-26258	Arcserve UDP through 9.0.6034 allows authentication bypass. The method getVersionInfo at WebServiceImpl/services/FlashServiceImpl leaks the AuthUUID token. This token can be used at /WebServiceImpl/services/VirtualStandbyServiceImpl to obtain a valid session. This session can be used to execute any task as administrator.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-22151	Permissions vulnerability in Fuel-CMS v.1.4.6 allows a remote attacker to execute arbitrary code via a crafted zip file to the assests parameter of the upload function.	9.8	More Details
CVE-2020-22153	File Upload vulnerability in FUEL-CMS v.1.4.6 allows a remote attacker to execute arbitrary code via a crafted .php file to the upload parameter in the navigation function.	9.8	More Details
CVE-2020-22597	An issue in Jerrscript- project Jerryscrip v. 2.3.0 allows a remote attacker to execute arbitrary code via the ecma_builtin_array_prototype_object_slice parameter.	9.8	More Details
CVE-2023-36258	An issue in LangChain before 0.0.236 allows an attacker to execute arbitrary code because Python code with os.system, exec, or eval can be used.	9.8	More Details
CVE-2023-36812	OpenTSDB is a open source, distributed, scalable Time Series Database (TSDB). OpenTSDB is vulnerable to Remote Code Execution vulnerability by writing user-controlled input to Gnuplot configuration file and running Gnuplot with the generated configuration. This issue has been patched in commit `07c4641471c` and further refined in commit `fa88d3e4b`. These patches are available in the `2.4.2` release. Users are advised to upgrade. User unable to upgrade may disable Gunuplot via the config option`tsd.core.enable_ui = true` and remove the shell files `mygnuplot.bat` and `mygnuplot.sh`.	9.8	More Details
CVE-2022-44720	An issue was discovered in Weblib Ucopia before 6.0.13. OS Command Injection injection can occur, related to chroot.	9.8	More Details
CVE-2023-35830	STW (aka Sensor-Technik Wiedemann) TCG-4 Connectivity Module DeploymentPackage_v3.03r0-Impala and DeploymentPackage_v3.04r2-Jellyfish and TCG-4lite Connectivity Module DeploymentPackage_v3.04r2-Jellyfish allow an attacker to gain full remote access with root privileges without the need for authentication, giving an attacker arbitrary remote code execution over LTE / 4G network via SMS.	9.8	More Details
CVE-2023-34487	itsourcecode Online Hotel Management System Project In PHP v1.0.0 is vulnerable to SQL Injection. SQL injection points exist in the login password input box. This vulnerability can be exploited through time-based blind injection.	9.8	More Details
CVE-2022-44276	In Responsive Filemanager < 9.12.0, an attacker can bypass upload restrictions resulting in RCE.	9.8	More Details
CVE-2023-21066	In cd_CodeMsg of cd_codec.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-250100597References: N/A	9.8	More Details
CVE-2021-25827	Emby Server < 4.7.12.0 is vulnerable to a login bypass attack by setting the X-Forwarded-For header to a local IP-address.	9.8	More Details
CVE-2023-33592	Lost and Found Information System v1.0 was discovered to contain a SQL injection vulnerability via the component /php-lfis/admin/?page=system_info/contact_information.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32222	D-Link DSL-G256DG version vBZ_1.00.27 web management interface allows authentication bypass via an unspecified method.	9.8	More Details
CVE-2023-32224	D-Link DSL-224 firmware version 3.0.10 CWE-307: Improper Restriction of Excessive Authentication Attempts	9.8	More Details
CVE-2023-36475	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 5.5.2 and 6.2.1, an attacker can use a prototype pollution sink to trigger a remote code execution through the MongoDB BSON parser. A patch is available in versions 5.5.2 and 6.2.1.	9.8	More Details
CVE-2023-31222	Deserialization of untrusted data in Microsoft Messaging Queuing Service in Medtronic's Paceart Optima versions 1.11 and earlier on Windows allows an unauthorized user to impact a healthcare delivery organization’s Paceart Optima system cardiac device causing data to be deleted, stolen, or modified, or the Paceart Optima system being used for further network penetration via network connectivity.	9.8	More Details
CVE-2023-2982	The WordPress Social Login and Register (Discord, Google, Twitter, LinkedIn) plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 7.6.4. This is due to insufficient encryption on the user being supplied during a login validated through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they know the email address associated with that user. This was partially patched in version 7.6.4 and fully patched in version 7.6.5.	9.8	More Details
CVE-2023-34738	Chemex through 3.7.1 is vulnerable to arbitrary file upload.	9.8	More Details
CVE-2023-34735	Property Cloud Platform Management Center 1.0 is vulnerable to error-based SQL injection.	9.8	More Details
CVE-2023-34598	Gibbon v25.0.0 is vulnerable to a Local File Inclusion (LFI) where it's possible to include the content of several files present in the installation folder in the server's response.	9.8	More Details
CVE-2023-34844	Play With Docker < 0.0.2 has an insecure CAP_SYS_ADMIN privileged mode causing the docker container to escape.	9.8	More Details
CVE-2023-34849	An unauthorized command injection vulnerability exists in the ActionLogin function of the webman.lua file in Ikuai router OS through 3.7.1.	9.8	More Details
CVE-2023-26612	D-Link DIR-823G firmware version 1.02B05 has a buffer overflow vulnerability, which originates from the HostName field in SetParentsControlInfo.	9.8	More Details
CVE-2023-26613	An OS command injection vulnerability in D-Link DIR-823G firmware version 1.02B05 allows unauthorized attackers to execute arbitrary operating system commands via a crafted GET request to EXCU_SHELL.	9.8	More Details
CVE-2023-26616	D-Link DIR-823G firmware version 1.02B05 has a buffer overflow vulnerability, which originates from the URL field in SetParentsControlInfo.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3460	The Ultimate Member WordPress plugin before 2.6.7 does not prevent visitors from creating user accounts with arbitrary capabilities, effectively allowing attackers to create administrator accounts at will. This is actively being exploited in the wild.	9.8	More Details
CVE-2023-20192	Multiple vulnerabilities in Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an authenticated attacker with Administrator-level read-only credentials to elevate their privileges to Administrator with read-write credentials on an affected system. Note: "Cisco Expressway Series" refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. For more information about these vulnerabilities, see the Details section of this advisory.	9.6	More Details
CVE-2023-20105	A vulnerability in the change password functionality of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an authenticated, remote attacker with Read-only credentials to elevate privileges to Administrator on an affected system. This vulnerability is due to incorrect handling of password change requests. An attacker could exploit this vulnerability by authenticating to the application as a Read-only user and sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to alter the passwords of any user on the system, including an administrative user, and then impersonate that user. Note: Cisco Expressway Series refers to the Expressway Control (Expressway-C) device and the Expressway Edge (Expressway-E) device.	9.6	More Details
CVE-2023-28365	A backup file vulnerability found in UniFi applications (Version 7.3.83 and earlier) running on Linux operating systems allows application administrators to execute malicious commands on the host device being restored.	9.1	More Details
CVE-2023-32623	Directory traversal vulnerability in Snow Monkey Forms v5.1.1 and earlier allows a remote unauthenticated attacker to delete arbitrary files on the server.	9.1	More Details
CVE-2023-36477	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with edit rights can edit all pages in the `CKEditor' space. This makes it possible to perform a variety of harmful actions, such as removing technical documents, leading to loss of service and editing the javascript configuration of CKEditor, leading to persistent XSS. This issue has been patched in XWiki 14.10.6 and XWiki 15.1. This issue has been patched on the CKEditor Integration extension 1.64.9 for XWiki version older than 14.6RC1. Users are advised to upgrade. Users unable to upgrade may manually address the issue by restricting the `edit` and `delete` rights to a trusted user or group (e.g. the `XWiki.XWikiAdminGroup` group), implicitly disabling those rights for all other users. See commit `9d9d86179` for details.	9.0	More Details
CVE-2023-31997	UniFi OS 3.1 introduces a misconfiguration on consoles running UniFi Network that allows users on a local network to access MongoDB. Applicable Cloud Keys that are both (1) running UniFi OS 3.1 and (2) hosting the UniFi Network application. "Applicable Cloud Keys" include the following: Cloud Key Gen2 and Cloud Key Gen2 Plus.	9.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36471	Xwiki commons is the common modules used by other XWiki top level projects. The HTML sanitizer that is included in XWiki since version 14.6RC1 allowed form and input HTML tags. In the context of XWiki, this allows an attacker without script right to either create forms that can be used for phishing attacks or also in the context of a sheet, the attacker could add an input like `{{html}} <input type="hidden" name="content" value="{{groovy}}println(&quot;Hello from Groovy!&quot;)" /> {{/html}}` that would allow remote code execution when it is submitted by an admin (the sheet is rendered as part of the edit form). The attacker would need to ensure that the edit form looks plausible, though, which can be non-trivial as without script right the attacker cannot display the regular content of the document. This has been patched in XWiki 14.10.6 and 15.2RC1 by removing the central form-related tags from the list of allowed tags. Users are advised to upgrade. As a workaround an admin can manually disallow the tags by adding `form, input, select, textarea, button` to the configuration option `xml.htmlElementSanitizer.forbidTags` in the `xwiki.properties` configuration file.	9.0	More Details
CVE-2023-2625	A vulnerability exists that can be exploited by an authenticated client that is connected to the same network segment as the CoreTec 4, having any level of access VIEWER to ADMIN. To exploit the vulnerability the attacker can inject shell commands through a particular field of the web user interface that will be executed by the system.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-31999	All versions of @fastify/oauth2 used a statically generated state parameter at startup time and were used across all requests for all users. The purpose of the Oauth2 state parameter is to prevent Cross-Site-Request-Forgery attacks. As such, it should be unique per user and should be connected to the user's session in some way that will allow the server to validate it. v7.2.0 changes the default behavior to store the state in a cookie with the http-only and same-site=lax attributes set. The state is now by default generated for every user. Note that this contains a breaking change in the checkStateFunction function, which now accepts the full Request object.	8.8	More Details
CVE-2023-33570	Bagisto v1.5.1 is vulnerable to Server-Side Template Injection (SSTI).	8.8	More Details
CVE-2023-33466	Orthanc before 1.12.0 allows authenticated users with access to the Orthanc API to overwrite arbitrary files on the file system, and in specific deployment scenarios allows the attacker to overwrite the configuration, which can be exploited to trigger Remote Code Execution (RCE).	8.8	More Details
CVE-2023-34656	An issue was discovered with the JSESSION IDs in Xiamen Si Xin Communication Technology Video management system 3.1 thru 4.1 allows attackers to gain escalated privileges.	8.8	More Details
CVE-2023-35178	Certain HP LaserJet Pro print products are potentially vulnerable to Buffer Overflow when performing a GET request to scan jobs.	8.8	More Details
CVE-2023-36162	Cross Site Request Forgery vulnerability in ZZCMS v.2023 and earlier allows a remote attacker to gain privileges via the add function in adminlist.php.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4401	The Style Kits plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.8.0. This is due to missing or incorrect nonce validation on the update_posts_stylekit() function. This makes it possible for unauthenticated attackers to update style kits for posts 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-2021-4398	The Amministrazione Trasparente plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 7.1. This is due to missing or incorrect nonce validation on the at_save_aturl_meta() function. This makes it possible for unauthenticated attackers to update meta data 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-2021-4394	The Locations plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.2.1. This is due to missing or incorrect nonce validation on the saveCustomFields() function. This makes it possible for unauthenticated attackers to update custom field meta data 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-2021-4386	The WP Security Question plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.0.5. This is due to missing or incorrect nonce validation on the save() function. This makes it possible for unauthenticated attackers to modify the plugin's settings 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-2021-4385	The WP Private Content Plus plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.1. This is due to missing or incorrect nonce validation on the save_groups() function. This makes it possible for unauthenticated attackers to add new group members 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-2023-36143	Maxprint Maxlink 1200G v3.4.11E has an OS command injection vulnerability in the "Diagnostic tool" functionality of the device.	8.8	More Details
CVE-2021-31982	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	8.8	More Details
CVE-2023-3063	The SP Project & Document Manager plugin for WordPress is vulnerable to Insecure Direct Object References in versions up to, and including, 4.67. This is due to the plugin providing user-controlled access to objects, letting a user bypass authorization and access system resources. This makes it possible for authenticated attackers with subscriber privileges or above, to change user passwords and potentially take over administrator accounts.	8.8	More Details
CVE-2023-35176	Certain HP LaserJet Pro print products are potentially vulnerable to Buffer Overflow and/or Denial of Service when using the backup & restore feature through the embedded web service on the device.	8.8	More Details
CVE-2023-3491	Unrestricted Upload of File with Dangerous Type in GitHub repository fossbilling/fossbilling prior to 0.5.3.	8.8	More Details
CVE-2023-35177	Certain HP LaserJet Pro print products are potentially vulnerable to a stack-based buffer overflow related to the compact font format parser.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22886	Improper Input Validation vulnerability in Apache Software Foundation Apache Airflow JDBC Provider. Airflow JDBC Provider Connection's [Connection URL] parameters had no restrictions, which made it possible to implement RCE attacks via different type JDBC drivers, obtain airflow server permission. This issue affects Apache Airflow JDBC Provider: before 4.0.0.	8.8	More Details
CVE-2023-22906	Hero Qubo HCD01_02_V1.38_20220125 devices allow TELNET access with root privileges by default, without a password.	8.8	More Details
CVE-2023-32223	D-Link DSL-224 firmware version 3.0.10 allows post authentication command execution via an unspecified method.	8.8	More Details
CVE-2023-1273	The ND Shortcodes WordPress plugin before 7.0 does not validate some shortcode attributes before using them to generate paths passed to include function/s, allowing any authenticated users such as subscriber to perform LFI attacks	8.8	More Details
CVE-2023-21517	Heap out-of-bound write vulnerability in Exynos baseband prior to SMR Jun-2023 Release 1 allows remote attacker to execute arbitrary code.	8.8	More Details
CVE-2023-30990	IBM i 7.2, 7.3, 7.4, and 7.5 could allow a remote attacker to execute CL commands as QUSER, caused by an exploitation of DDM architecture. IBM X-Force ID: 254036.	8.6	More Details
CVE-2023-3447	The Active Directory Integration / LDAP Integration plugin for WordPress is vulnerable to LDAP Injection in versions up to, and including, 4.1.5. This is due to insufficient escaping on the supplied username value. This makes it possible for unauthenticated attackers to extract potentially sensitive information from the LDAP directory.	8.6	More Details
CVE-2023-20006	A vulnerability in the hardware-based SSL/TLS cryptography functionality of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 2100 Series Appliances could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to an implementation error within the cryptographic functions for SSL/TLS traffic processing when they are offloaded to the hardware. An attacker could exploit this vulnerability by sending a crafted stream of SSL/TLS traffic to an affected device. A successful exploit could allow the attacker to cause an unexpected error in the hardware-based cryptography engine, which could cause the device to reload.	8.6	More Details
CVE-2023-21672	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions.	8.4	More Details
CVE-2023-22667	Memory Corruption in Audio while allocating the ion buffer during the music playback.	8.4	More Details
CVE-2022-29146	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3243	** UNSUPPORTED WHEN ASSIGNED ** [An attacker can capture an authenticating hash and utilize it to create new sessions. The hash is also a poorly salted MD5 hash, which could result in a successful brute force password attack. Impacted product is BCM-WEB version 3.3.X. Recommended fix: Upgrade to a supported product such as Alerton ACM.] Out of an abundance of caution, this CVE ID is being assigned to better serve our customers and ensure all who are still running this product understand that the product is end of life and should be removed or upgraded.	8.3	More Details
CVE-2023-34451	CometBFT is a Byzantine Fault Tolerant (BFT) middleware that takes a state transition machine and replicates it on many machines. The mempool maintains two data structures to keep track of outstanding transactions: a list and a map. These two data structures are supposed to be in sync all the time in the sense that the map tracks the index (if any) of the transaction in the list. In `v0.37.0`, and `v0.37.1`, as well as in `v0.34.28`, and all previous releases of the CometBFT repo2, it is possible to have them out of sync. When this happens, the list may contain several copies of the same transaction. Because the map tracks a single index, it is then no longer possible to remove all the copies of the transaction from the list. This happens even if the duplicated transaction is later committed in a block. The only way to remove the transaction is by restarting the node. The above problem can be repeated on and on until a sizable number of transactions are stuck in the mempool, in order to try to bring down the target node. The problem is fixed in releases `v0.34.29` and `v0.37.2`. Some workarounds are available. Increasing the value of `cache_size` in `config.toml` makes it very difficult to effectively attack a full node. Not exposing the transaction submission RPC's would mitigate the probability of a successful attack, as the attacker would then have to create a modified (byzantine) full node to be able to perform the attack via p2p.	8.2	More Details
CVE-2023-36474	Interactsh is an open-source tool for detecting out-of-band interactions. Domains configured with interactsh server prior to version 1.0.0 were vulnerable to subdomain takeover for a specific subdomain, i.e `app.` Interactsh server used to create cname entries for `app` pointing to `projectdiscovery.github.io` as default, which intended to used for hosting interactsh web client using GitHub pages. This is a security issue with a self-hosted interactsh server in which the user may not have configured a web client but still have a CNAME entry pointing to GitHub pages, making them vulnerable to subdomain takeover. This allows a threat actor to host / run arbitrary client side code (cross-site scripting) in a user's browser when browsing the vulnerable subdomain. Version 1.0.0 fixes this issue by making CNAME optional, rather than default.	8.2	More Details
CVE-2021-31937	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	8.2	More Details
CVE-2023-3314	A vulnerability arises out of a failure to comprehensively sanitize the processing of a zip file(s). Incomplete neutralization of external commands used to control the process execution of the .zip application allows an authorized user to obtain control of the .zip application to execute arbitrary commands or obtain elevation of system privileges.	8.1	More Details
CVE-2023-29241	Improper Information in Cybersecurity Guidebook in Bosch Building Integration System (BIS) 5.0 may lead to wrong configuration which allows local users to access data via network	8.1	More Details
CVE-2023-32613	Exposure of resource to wrong sphere issue exists in WL-WN531AX2 firmware versions prior to 2023526, which may allow a network-adjacent attacker to use functions originally available after login without logging in.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36467	AWS data.all is an open source development framework to help users build a data marketplace on Amazon Web Services. data.all versions 1.2.0 through 1.5.1 do not prevent remote code execution when a user injects Python commands into the 'Template' field when configuring a data pipeline. The issue can only be triggered by authenticated users. A fix for this issue is available in data.all version 1.5.2 and later. There is no recommended work around.	8.0	More Details
CVE-2023-3493	Improper Neutralization of Formula Elements in a CSV File in GitHub repository fossbilling/fossbilling prior to 0.5.3.	8.0	More Details
CVE-2023-36476	calamares-nixos-extensions provides Calamares branding and modules for NixOS, a distribution of GNU/Linux. Users of calamares-nixos-extensions version 0.3.12 and prior who installed NixOS through the graphical calamares installer, with an unencrypted `/boot`, on either non-UEFI systems or with a LUKS partition different from `/` have their LUKS key file in `/boot` as a plaintext CPIO archive attached to their NixOS initrd. A patch is available and anticipated to be part of version 0.3.13 to backport to NixOS 22.11, 23.05, and unstable channels. Expert users who have a copy of their data may, as a workaround, re-encrypt the LUKS partition(s) themselves.	7.9	More Details
CVE-2023-1295	A time-of-check to time-of-use issue exists in io_uring subsystem's IORING_OP_CLOSE operation in the Linux kernel's versions 5.6 - 5.11 (inclusive), which allows a local user to elevate their privileges to root. Introduced in b5dba59e0cf7e2cc4d3b3b1ac5fe81ddf21959eb, patched in 9eac1904d3364254d622bf2c771c4f85cd435fc2, backported to stable in 788d0824269bef539fe31a785b1517882eafed93.	7.8	More Details
CVE-2023-21175	In onCreate of DataUsageSummary.java, there is a possible method for a guest user to enable or disable mobile data due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262243574	7.8	More Details
CVE-2023-21174	In isPageSearchEnabled of BillingCycleSettings.java, there is a possible way for the guest user to change data limits due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-235822222	7.8	More Details
CVE-2023-22387	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	7.8	More Details
CVE-2023-21179	In parseSecurityParamsFromXml of XmlUtil.java, there is a possible bypass of user specified wifi encryption protocol due to improperly used crypto. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-272755865	7.8	More Details
CVE-2023-21172	In multiple functions of WifiCallingSettings.java, there is a possible way to change calling preferences for the admin user due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262243015	7.8	More Details
CVE-2023-24851	Memory Corruption in WLAN HOST while parsing QMI response message from firmware.	7.8	More Details
CVE-2023-28541	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3313	An OS common injection vulnerability exists in the ESM certificate API, whereby incorrectly neutralized special elements may have allowed an unauthorized user to execute system command injection for the purpose of privilege escalation or to execute arbitrary commands.	7.8	More Details
CVE-2023-24854	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message.	7.8	More Details
CVE-2023-21187	In onCreate of UsbAccessoryUriActivity.java, there is a possible way to escape the Setup Wizard due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246542917	7.8	More Details
CVE-2023-21183	In ForegroundUtils of ForegroundUtils.java, there is a possible way to read NFC tag data while the app is still in the background due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-235863754	7.8	More Details
CVE-2023-36183	Buffer Overflow vulnerability in OpenImageIO v.2.4.12.0 and before allows a remote to execute arbitrary code and obtain sensitive information via a crafted file to the readimg function.	7.8	More Details
CVE-2022-20443	In hasInputInfo of Layer.cpp, there is a possible bypass of user interaction requirements due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-194480991	7.8	More Details
CVE-2023-21191	In fixNotification of NotificationManagerService.java, there is a possible bypass of notification hide preference due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-269738057	7.8	More Details
CVE-2023-29145	The Malwarebytes EDR 1.0.11 for Linux driver doesn't properly ensure whitelisting of executable libraries loaded by executable files, allowing arbitrary code execution. The attacker can set LD_LIBRARY_PATH, set LD_PRELOAD, or run an executable file in a debugger.	7.8	More Details
CVE-2023-20773	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735.	7.8	More Details
CVE-2023-3389	A use-after-free vulnerability in the Linux Kernel io_uring subsystem can be exploited to achieve local privilege escalation. Racing a io_uring cancel poll request with a linked timeout can cause a UAF in a hrtimer. We recommend upgrading past commit ef7dfac51d8ed961b742218f526bd589f3900a59 (4716c73b188566865bdd79c3a6709696a224ac04 for 5.10 stable and 0e388fce7aec40992eadee654193cad345d62663 for 5.15 stable).	7.8	More Details
CVE-2023-20178	A vulnerability in the client update process of Cisco AnyConnect Secure Mobility Client Software for Windows and Cisco Secure Client Software for Windows could allow a low-privileged, authenticated, local attacker to elevate privileges to those of SYSTEM. The client update process is executed after a successful VPN connection is established. This vulnerability exists because improper permissions are assigned to a temporary directory that is created during the update process. An attacker could exploit this vulnerability by abusing a specific function of the Windows installer process. A successful exploit could allow the attacker to execute code with SYSTEM privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3090	A heap out-of-bounds write vulnerability in the Linux Kernel ipvlan network driver can be exploited to achieve local privilege escalation. The out-of-bounds write is caused by missing skb->cb initialization in the ipvlan network driver. The vulnerability is reachable if CONFIG_IPVLAN is enabled. We recommend upgrading past commit 90cbed5247439a966b645b34eb0a2e037836ea8e.	7.8	More Details
CVE-2023-22386	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory.	7.8	More Details
CVE-2023-3390	A use-after-free vulnerability was found in the Linux kernel's netfilter subsystem in net/netfilter/nf_tables_api.c. Mishandled error handling with NFT_MSG_NEWRULE makes it possible to use a dangling pointer in the same transaction causing a use-after-free vulnerability. This flaw allows a local attacker with user access to cause a privilege escalation issue. We recommend upgrading past commit 1240eb93f0616b21c675416516ff3d74798fdc97.	7.8	More Details
CVE-2023-26085	A possible out-of-bounds read and write (due to an improper length check of shared memory) was discovered in Arm NN Android-NN-Driver before 23.02.	7.8	More Details
CVE-2023-21184	In getCurrentPrivilegedPackagesForAllUsers of CarrierPrivilegesTracker.java, there is a possible permission bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-267809568	7.8	More Details
CVE-2023-21225	there is a possible way to bypass the protected confirmation screen due to Failure to lock display power. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-270403821References: N/A	7.8	More Details
CVE-2023-21147	In lwis_i2c_device_disable of lwis_device_i2c.c, there is a possible UAF due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-269661912References: N/A	7.8	More Details
CVE-2023-21149	In registerGsmaServiceIntentReceiver of ShannonRcsService.java, there is a possible way to activate/deactivate RCS service due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-270050709References: N/A	7.8	More Details
CVE-2023-33298	com.perimeter81.osx.HelperTool in Perimeter81 10.0.0.19 on macOS allows Local Privilege Escalation (to root) via shell metacharacters in usingCAPath.	7.8	More Details
CVE-2023-28542	Memory Corruption in WLAN HOST while fetching TX status information.	7.8	More Details
CVE-2023-36377	Buffer Overflow vulnerability in mtrojnar osslsigncode v.2.3 and before allows a local attacker to execute arbitrary code via a crafted .exe, .sys, and .dll files.	7.8	More Details
CVE-2023-21185	In multiple functions of WifiNetworkFactory.java, there is a missing permission check. This could lead to local escalation of privilege from the guest user with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-266700762	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21192	In setInputMethodWithSubtypeIdLocked of InputMethodManagerService.java, there is a possible way to setup input methods that are not enabled due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-227207653	7.8	More Details
CVE-2023-2846	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series main modules allows a remote unauthenticated attacker to cancel the password/keyword setting and login to the affected products by sending specially crafted packets.	7.5	More Details
CVE-2020-26709	py-xml v1.0 was discovered to contain an XML External Entity Injection (XXE) vulnerability which allows attackers to execute arbitrary code via a crafted XML file.	7.5	More Details
CVE-2023-36347	A broken authentication mechanism in the endpoint excel.php of POS Codekop v2.0 allows unauthenticated attackers to download selling data.	7.5	More Details
CVE-2020-26710	easy-parse v0.1.1 was discovered to contain a XML External Entity Injection (XXE) vulnerability which allows attackers to execute arbitrary code via a crafted XML file.	7.5	More Details
CVE-2020-26708	requests-xml v0.2.3 was discovered to contain an XML External Entity Injection (XXE) vulnerability which allows attackers to execute arbitrary code via a crafted XML file.	7.5	More Details
CVE-2023-21219	there is a possible use of unencrypted transport over cellular networks due to an insecure default value. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-264698379References: N/A	7.5	More Details
CVE-2023-21220	there is a possible use of unencrypted transport over cellular networks due to an insecure default value. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-264590585References: N/A	7.5	More Details
CVE-2022-44719	An issue was discovered in Weblib Ucopia before 6.0.13. The SSH Server has Insecure Permissions.	7.5	More Details
CVE-2023-34843	Traggo Server 0.3.0 is vulnerable to directory traversal via a crafted GET request.	7.5	More Details
CVE-2022-29144	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	7.5	More Details
CVE-2023-21223	In LPP_ConvertGNSS_DataBitAssistance of LPP_CommonUtil.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-256047000References: N/A	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21224	In ss_ProcessReturnResultComponent of ss_MmConManagement.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-265276966References: N/A	7.5	More Details
CVE-2023-21226	In SAEMM_RetrieveTaiList of SAEMM_ContextManagement.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-240728187References: N/A	7.5	More Details
CVE-2023-33277	The web interface of Gira Giersiepen Gira KNX/IP-Router 3.1.3683.0 and 3.3.8.0 allows a remote attacker to read sensitive files via directory-traversal sequences in the URL.	7.5	More Details
CVE-2023-32610	Mailform Pro CGI 4.3.1.2 and earlier allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition.	7.5	More Details
CVE-2023-21201	In on_create_record_event of btif_sdp_server.cc, there is a possible out of bounds read due to a missing null check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-263545186	7.5	More Details
CVE-2023-30589	The llhttp parser in the http module in Node v20.2.0 does not strictly use the CRLF sequence to delimit HTTP requests. This can lead to HTTP Request Smuggling (HRS). The CR character (without LF) is sufficient to delimit HTTP header fields in the llhttp parser. According to RFC7230 section 3, only the CRLF sequence should delimit each header-field. This impacts all Node.js active versions: v16, v18, and, v20	7.5	More Details
CVE-2023-37306	MISP 2.4.172 mishandles different certificate file extensions in server sync. An attacker can obtain sensitive information because of the nature of the error messages.	7.5	More Details
CVE-2023-21197	In btm_acl_process_sca_cmpl_pkt of btm_acl.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-251427561	7.5	More Details
CVE-2023-34936	A stack overflow in the UpdateMacClone function of H3C Magic B1STV100R012 allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	7.5	More Details
CVE-2023-34935	A stack overflow in the AddWlanMacList function of H3C Magic B1STV100R012 allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	7.5	More Details
CVE-2023-34934	A stack overflow in the Edit_BasicSSID_5G function of H3C Magic B1STV100R012 allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	7.5	More Details
CVE-2023-34933	A stack overflow in the UpdateWanParams function of H3C Magic B1STV100R012 allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	7.5	More Details
CVE-2023-26615	D-Link DIR-823G firmware version 1.02B05 has a password reset vulnerability, which originates from the SetMultipleActions API, allowing unauthorized attackers to reset the WEB page management password.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20690	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664735; Issue ID: ALPS07664735.	7.5	More Details
CVE-2023-20691	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664731; Issue ID: ALPS07664731.	7.5	More Details
CVE-2023-20692	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664720; Issue ID: ALPS07664720.	7.5	More Details
CVE-2023-20693	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664711; Issue ID: ALPS07664711.	7.5	More Details
CVE-2023-21631	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network.	7.5	More Details
CVE-2023-20108	A vulnerability in the XCP Authentication Service of the Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) could allow an unauthenticated, remote attacker to cause a temporary service outage for all Cisco Unified CM IM&P users who are attempting to authenticate to the service, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted login message to the affected device. A successful exploit could allow the attacker to cause an unexpected restart of the authentication service, preventing new users from successfully authenticating. Exploitation of this vulnerability does not impact Cisco Unified CM IM&P users who were authenticated prior to an attack.	7.5	More Details
CVE-2023-34932	A stack overflow in the UpdateWanMode function of H3C Magic B1STV100R012 allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	7.5	More Details
CVE-2023-34931	A stack overflow in the EditWlanMacList function of H3C Magic B1STV100R012 allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	7.5	More Details
CVE-2023-34930	A stack overflow in the EditMacList function of H3C Magic B1STV100R012 allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	7.5	More Details
CVE-2023-34929	A stack overflow in the AddMacList function of H3C Magic B1STV100R012 allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	7.5	More Details
CVE-2023-34928	A stack overflow in the Edit_BasicSSID function of H3C Magic B1STV100R012 allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	7.5	More Details
CVE-2023-3133	The Tutor LMS WordPress plugin before 2.2.1 does not implement adequate permission checks for REST API endpoints, allowing unauthenticated attackers to access information from Lessons that should not be publicly available.	7.5	More Details
CVE-2023-34937	A stack overflow in the UpdateSnat function of H3C Magic B1STV100R012 allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20689	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664741; Issue ID: ALPS07664741.	7.5	More Details
CVE-2022-32666	In Wi-Fi, there is a possible low throughput due to misrepresentation of critical information. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220829014; Issue ID: GN20220829014.	7.5	More Details
CVE-2023-36053	In Django 3.2 before 3.2.20, 4 before 4.1.10, and 4.2 before 4.2.3, EmailValidator and URLValidator are subject to a potential ReDoS (regular expression denial of service) attack via a very large number of domain name labels of emails and URLs.	7.5	More Details
CVE-2023-21193	In VideoFrame of VideoFrame.h, there is a possible abort due to an integer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-233006499	7.5	More Details
CVE-2023-36144	An authentication bypass in Intelbras Switch SG 2404 MR in firmware 1.00.54 allows an unauthenticated attacker to download the backup file of the device, exposing critical information about the device configuration.	7.5	More Details
CVE-2023-21186	In LogResponse of Dns.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261079188	7.5	More Details
CVE-2023-25522	NVIDIA DGX A100/A800 contains a vulnerability in SBIOS where an attacker may cause improper input validation by providing configuration information in an unexpected format. A successful exploit of this vulnerability may lead to denial of service, information disclosure, and data tampering.	7.5	More Details
CVE-2023-21180	In xmlParseTryOrFinish of parser.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261365944	7.5	More Details
CVE-2023-30586	A privilege escalation vulnerability exists in Node.js 20 that allowed loading arbitrary OpenSSL engines when the experimental permission model is enabled, which can bypass and/or disable the permission model. The attack complexity is high. However, the crypto.setEngine() API can be used to bypass the permission model when called with a compatible OpenSSL engine. The OpenSSL engine can, for example, disable the permission model in the host process by manipulating the process's stack memory to locate the permission model Permission::enabled_ in the host process's heap memory. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.	7.5	More Details
CVE-2023-26509	AnyDesk 7.0.8 allows remote Denial of Service.	7.5	More Details
CVE-2023-36814	Products.CMFCore are the key framework services for the Zope Content Management Framework (CMF). The use of Python's marshal module to handle unchecked input in a public method on `PortalFolder` objects can lead to an unauthenticated denial of service and crash situation. The code in question is exposed by all portal software built on top of `Products.CMFCore`, such as Plone. All deployments are vulnerable. The code has been fixed in `Products.CMFCore` version 3.2.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36817	`tktchurch/website` contains the codebase for The King's Temple Church website. In version 0.1.0, a Stripe API key was found in the public code repository of the church's project. This sensitive information was unintentionally committed and subsequently exposed in the codebase. If an unauthorized party gains access to this key, they could potentially carry out transactions on behalf of the organization, leading to financial losses. Additionally, they could access sensitive customer information, leading to privacy violations and potential legal implications. The affected component is the codebase of our project, specifically the file(s) where the Stripe API key is embedded. The key should have been stored securely, and not committed to the codebase. The maintainers plan to revoke the leaked Stripe API key immediately, generate a new one, and not commit the key to the codebase.	7.5	More Details
CVE-2023-25521	NVIDIA DGX A100/A800 contains a vulnerability in SBIOS where an attacker may cause execution with unnecessary privileges by leveraging a weakness whereby proper input parameter validation is not performed. A successful exploit of this vulnerability may lead to denial of service, information disclosure, and data tampering.	7.5	More Details
CVE-2023-3138	A vulnerability was found in libX11. The security flaw occurs because the functions in src/InitExt.c in libX11 do not check that the values provided for the Request, Event, or Error IDs are within the bounds of the arrays that those functions write to, using those IDs as array indexes. They trust that they were called with values provided by an Xserver adhering to the bounds specified in the X11 protocol, as all X servers provided by X.Org do. As the protocol only specifies a single byte for these values, an out-of-bounds value provided by a malicious server (or a malicious proxy-in-the-middle) can only overwrite other portions of the Display structure and not write outside the bounds of the Display structure itself, possibly causing the client to crash with this memory corruption.	7.5	More Details
CVE-2023-36815	Sealos is a Cloud Operating System designed for managing cloud-native applications. In version 4.2.0 and prior, there is a permission flaw in the Sealos billing system, which allows users to control the recharge resource account `sealos[.] io/v1/Payment`, resulting in the ability to recharge any amount of 1 renminbi (RMB). The charging interface may expose resource information. The namespace of this custom resource would be user's control and may have permission to correct it. It is not clear whether a fix exists.	7.3	More Details
CVE-2023-26135	All versions of the package flatnest are vulnerable to Prototype Pollution via the nest() function in the flatnest/nest.js file.	7.3	More Details
CVE-2023-21189	In startLockTaskMode of LockTaskController.java, there is a possible bypass of lock task mode due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-213942596	7.3	More Details
CVE-2023-36609	The affected TBox RTUs run OpenVPN with root privileges and can run user defined configuration scripts. An attacker could set up a local OpenVPN server and push a malicious script onto the TBox host to acquire root privileges.	7.2	More Details
CVE-2023-32612	Client-side enforcement of server-side security issue exists in WL-WN531AX2 firmware versions prior to 2023526, which may allow an attacker with an administrative privilege to execute OS commands with the root privilege.	7.2	More Details
CVE-2023-32621	WL-WN531AX2 firmware versions prior to 2023526 allows an attacker with an administrative privilege to upload arbitrary files and execute OS commands with the root privilege.	7.2	More Details
CVE-2023-34736	Guantang Equipment Management System version 4.12 is vulnerable to Arbitrary File Upload.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32622	Improper neutralization of special elements in WL-WN531AX2 firmware versions prior to 2023526 allows an attacker with an administrative privilege to execute OS commands with the root privilege.	7.2	More Details
CVE-2023-3333	Improper Neutralization of Special Elements used in an OS Command vulnerability in NEC Corporation Aterm WG2600HP2, WG2600HP, WG2200HP, WG1800HP2, WG1800HP, WG1400HP, WG600HP, WG300HP, WF300HP, WR9500N, WR9300N, WR8750N, WR8700N, WR8600N, WR8370N, WR8175N and WR8170N all versions allows a attacker to execute an arbitrary OS command with the root privilege, after obtaining a high privilege exploiting CVE-2023-3330 and CVE-2023-3331 vulnerabilities.	7.2	More Details
CVE-2023-25516	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where an unprivileged user can cause an integer overflow, which may lead to information disclosure and denial of service.	7.1	More Details
CVE-2023-27469	Malwarebytes Anti-Exploit 4.4.0.220 is vulnerable to arbitrary file deletion and denial of service via an ALPC message in which FullFileNamePath lacks a '\0' character.	7.1	More Details
CVE-2023-25517	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where a guest OS may be able to control resources for which it is not authorized, which may lead to information disclosure and data tampering.	7.1	More Details
CVE-2023-26299	A potential Time-of-Check to Time-of-Use (TOCTOU) vulnerability has been identified in certain HP PC products using AMI UEFI Firmware (system BIOS), which might allow arbitrary code execution. AMI has released updates to mitigate the potential vulnerability.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35947	Gradle is a build tool with a focus on build automation and support for multi-language development. In affected versions when unpacking Tar archives, Gradle did not check that files could be written outside of the unpack location. This could lead to important files being overwritten anywhere the Gradle process has write permissions. For a build reading Tar entries from a Tar archive, this issue could allow Gradle to disclose information from sensitive files through an arbitrary file read. To exploit this behavior, an attacker needs to either control the source of an archive already used by the build or modify the build to interact with a malicious archive. It is unlikely that this would go unnoticed. A fix has been released in Gradle 7.6.2 and 8.2 to protect against this vulnerability. Starting from these versions, Gradle will refuse to handle Tar archives which contain path traversal elements in a Tar entry name. Users are advised to upgrade. There are no known workarounds for this vulnerability. ### Impact This is a path traversal vulnerability when Gradle deals with Tar archives, often referenced as TarSlip, a variant of ZipSlip. * When unpacking Tar archives, Gradle did not check that files could be written outside of the unpack location. This could lead to important files being overwritten anywhere the Gradle process has write permissions. * For a build reading Tar entries from a Tar archive, this issue could allow Gradle to disclose information from sensitive files through an arbitrary file read. To exploit this behavior, an attacker needs to either control the source of an archive already used by the build or modify the build to interact with a malicious archive. It is unlikely that this would go unnoticed. Gradle uses Tar archives for its [Build Cache](https://docs.gradle.org/current/userguide/build_cache.html). These archives are safe when created by Gradle. But if an attacker had control of a remote build cache server, they could inject malicious build cache entries that leverage this vulnerability. This attack vector could also be exploited if a man-in-the-middle can be performed between the remote cache and the build. ### Patches A fix has been released in Gradle 7.6.2 and 8.2 to protect against this vulnerability. Starting from these versions, Gradle will refuse to handle Tar archives which contain path traversal elements in a Tar entry name. It is recommended that users upgrade to a patched version. ### Workarounds There is no workaround. * If your build deals with Tar archives that you do not fully trust, you need to inspect them to confirm they do not attempt to leverage this vulnerability. * If you use the Gradle remote build cache, make sure only trusted parties have write access to it and that connections to the remote cache are properly secured. ### References * [CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')](https://cwe.mitre.org/data/definitions/22.html) * [Gradle Build Cache](https://docs.gradle.org/current/userguide/build_cache.html) * [ZipSlip](https://security.snyk.io/research/zip-slip-vulnerability)	6.9	More Details
CVE-2023-35946	Gradle is a build tool with a focus on build automation and support for multi-language development. When Gradle writes a dependency into its dependency cache, it uses the dependency's coordinates to compute a file location. With specially crafted dependency coordinates, Gradle can be made to write files into an unintended location. The file may be written outside the dependency cache or over another file in the dependency cache. This vulnerability could be used to poison the dependency cache or overwrite important files elsewhere on the filesystem where the Gradle process has write permissions. Exploiting this vulnerability requires an attacker to have control over a dependency repository used by the Gradle build or have the ability to modify the build's configuration. It is unlikely that this would go unnoticed. A fix has been released in Gradle 7.6.2 and 8.2 to protect against this vulnerability. Gradle will refuse to cache dependencies that have path traversal elements in their dependency coordinates. It is recommended that users upgrade to a patched version. If you are unable to upgrade to Gradle 7.6.2 or 8.2, `dependency verification` will make this vulnerability more difficult to exploit.	6.9	More Details
CVE-2023-21629	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20116	A vulnerability in the Administrative XML Web Service (AXL) API of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of user-supplied input to the web UI of the Self Care Portal. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to cause a DoS condition on the affected device.	6.8	More Details
CVE-2022-46408	Ericsson Network Manager (ENM), versions prior to 22.1, contains a vulnerability in the application Network Connectivity Manager (NCM) where improper Neutralization of Formula Elements in a CSV File can lead to remote code execution or data leakage via maliciously injected hyperlinks. The attacker would need admin/elevated access to exploit the vulnerability.	6.8	More Details
CVE-2023-20760	In apu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629578; Issue ID: ALPS07629578.	6.7	More Details
CVE-2023-21203	In startWpsPbcInternal of sta_iface.cpp, there is a possible out of bounds read due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262246082	6.7	More Details
CVE-2023-21222	In load_dt_data of storage.c, 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.Product: AndroidVersions: Android kernelAndroid ID: A-266977723References: N/A	6.7	More Details
CVE-2023-20761	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582.	6.7	More Details
CVE-2023-21153	In Do_AIMS_SET_CALL_WAITING of imsservice.cpp, there is a possible out of bounds read 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.Product: AndroidVersions: Android kernelAndroid ID: A-264259730References: N/A	6.7	More Details
CVE-2023-21236	In aoc_service_set_read_blocked of aoc.c, 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.Product: AndroidVersions: Android kernelAndroid ID: A-270148537References: N/A	6.7	More Details
CVE-2023-20772	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796.	6.7	More Details
CVE-2023-20757	In cmdq, 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: ALPS07636133; Issue ID: ALPS07636133.	6.7	More Details
CVE-2023-21146	there is a possible way to corrupt memory 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.Product: AndroidVersions: Android kernelAndroid ID: A-239867994References: N/A	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21151	In the Google BMS kernel module, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-265149414References: N/A	6.7	More Details
CVE-2023-20767	In pqframework, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629585; Issue ID: ALPS07629584.	6.7	More Details
CVE-2023-21209	In multiple functions of sta_iface.cpp, there is a possible out of bounds read due to unsafe deserialization. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262236273	6.7	More Details
CVE-2023-20753	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667.	6.7	More Details
CVE-2023-21207	In initiateTdlsSetupInternal of sta_iface.cpp, there is a possible out of bounds read 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.Product: AndroidVersions: Android-13Android ID: A-262236670	6.7	More Details
CVE-2023-20754	In keyinstall, 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: ALPS07563028; Issue ID: ALPS07588343.	6.7	More Details
CVE-2023-20755	In keyinstall, 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: ALPS07510064; Issue ID: ALPS07509605.	6.7	More Details
CVE-2023-21640	Memory corruption in Linux when the file upload API is called with parameters having large buffer.	6.7	More Details
CVE-2023-20756	In keyinstall, 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: ALPS07510064; Issue ID: ALPS07549928.	6.7	More Details
CVE-2023-21639	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client.	6.7	More Details
CVE-2023-21638	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization.	6.7	More Details
CVE-2023-21637	Memory corruption in Linux while calling system configuration APIs.	6.7	More Details
CVE-2023-21635	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony.	6.7	More Details
CVE-2023-20766	In gps, 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: ALPS07573237; Issue ID: ALPS07573202.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21633	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request.	6.7	More Details
CVE-2023-20775	In display, 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: ALPS07978760; Issue ID: ALPS07363410.	6.7	More Details
CVE-2023-21171	In verifyInputEvent of InputDispatcher.cpp, there is a possible way to conduct click fraud due to side channel information disclosure. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261085213	6.7	More Details
CVE-2023-20774	In display, there is a possible out of bounds read 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: ALPS07292228; Issue ID: ALPS07292228.	6.7	More Details
CVE-2023-21161	In Parse of simdata.cpp, 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.Product: AndroidVersions: Android kernelAndroid ID: A-263783702References: N/A	6.7	More Details
CVE-2023-21159	In Parse of simdata.cpp, 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.Product: AndroidVersions: Android kernelAndroid ID: A-263783565References: N/A	6.7	More Details
CVE-2023-20768	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800.	6.7	More Details
CVE-2023-21157	In encode of wlandata.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-263783137References: N/A	6.7	More Details
CVE-2023-21641	An app with non-privileged access can change global system brightness and cause undesired system behavior.	6.6	More Details
CVE-2023-36611	The affected TBox RTUs allow low privilege users to access software security tokens of higher privilege. This could allow an attacker with “user” privileges to access files requiring higher privileges by establishing an SSH session and providing the other tokens.	6.5	More Details
CVE-2023-2232	An issue has been discovered in GitLab affecting all versions starting from 15.10 before 16.1, leading to a ReDoS vulnerability in the Jira prefix	6.5	More Details
CVE-2023-26136	Versions of the package tough-cookie before 4.1.3 are vulnerable to Prototype Pollution due to improper handling of Cookies when using CookieJar in rejectPublicSuffixes=false mode. This issue arises from the manner in which the objects are initialized.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37237	In Veritas NetBackup Appliance before 4.1.0.1 MR3, insecure permissions may allow an authenticated Admin to bypass shell restrictions and execute arbitrary operating system commands via SSH.	6.5	More Details
CVE-2023-37365	Hnswlib 0.7.0 has a double free in init_index when the M argument is a large integer.	6.5	More Details
CVE-2023-2728	Users may be able to launch containers that bypass the mountable secrets policy enforced by the ServiceAccount admission plugin when using ephemeral containers. The policy ensures pods running with a service account may only reference secrets specified in the service account's secrets field. Kubernetes clusters are only affected if the ServiceAccount admission plugin and the `kubernetes.io/enforce-mountable-secrets` annotation are used together with ephemeral containers.	6.5	More Details
CVE-2023-3395	All versions of the TWinSoft Configuration Tool store encrypted passwords as plaintext in memory. An attacker with access to system files could open a file to load the document into memory, including sensitive information associated with document, such as password. The attacker could then obtain the plaintext password by using a memory viewer.	6.5	More Details
CVE-2023-36819	Knowage is the professional open source suite for modern business analytics over traditional sources and big data systems. The endpoint `_/knowage/restful-services/dossier/importTemplateFile_` allows authenticated users to download template hosted on the server. However, starting in the 6.x.x branch and prior to version 8.1.8, the application does not sanitize the `_templateName_ `parameter allowing an attacker to use `*../*` in it, and escaping the directory the template are normally placed and download any file from the system. This vulnerability allows a low privileged attacker to exfiltrate sensitive configuration file. This issue has been patched in Knowage version 8.1.8.	6.5	More Details
CVE-2023-32608	Directory traversal vulnerability in Pleasanter (Community Edition and Enterprise Edition) 1.3.39.2 and earlier versions allows a remote authenticated attacker to alter an arbitrary file on the server.	6.5	More Details
CVE-2023-2974	A vulnerability was found in quarkus-core. This vulnerability occurs because the TLS protocol configured with quarkus.http.ssl.protocols is not enforced, and the client can force the selection of the weaker supported TLS protocol.	6.5	More Details
CVE-2023-36608	The affected TBox RTUs store hashed passwords using MD5 encryption, which is an insecure encryption algorithm.	6.5	More Details
CVE-2023-32620	Improper authentication vulnerability in WL-WN531AX2 firmware versions prior to 2023526 allows a network-adjacent attacker to obtain a password for the wireless network.	6.5	More Details
CVE-2023-34761	An unauthenticated attacker within BLE proximity can remotely connect to a 7-Eleven LED Message Cup, Hello Cup 1.3.1 for Android, and bypass the application's client-side chat censor filter.	6.5	More Details
CVE-2015-1313	JetBrains TeamCity 8 and 9 before 9.0.2 allows bypass of account-creation restrictions via a crafted request because the required request data can be deduced by reading HTML and JavaScript files that are returned to the web browser after an initial unauthenticated request.	6.5	More Details
CVE-2023-2727	Users may be able to launch containers using images that are restricted by ImagePolicyWebhook when using ephemeral containers. Kubernetes clusters are only affected if the ImagePolicyWebhook admission plugin is used together with ephemeral containers.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3338	A null pointer dereference flaw was found in the Linux kernel's DECnet networking protocol. This issue could allow a remote user to crash the system.	6.5	More Details
CVE-2023-20771	In display, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671046; Issue ID: ALPS07671046.	6.4	More Details
CVE-2022-4143	An issue has been discovered in GitLab affecting all versions starting from 15.7 before 15.8.5, from 15.9 before 15.9.4, and from 15.10 before 15.10.1 that allows for crafted, unapproved MRs to be introduced and merged without authorization	6.4	More Details
CVE-2023-3503	A vulnerability has been found in SourceCodester Shopping Website 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file insert-product.php. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-232951.	6.3	More Details
CVE-2023-3504	A vulnerability was found in SmartWeb Infotech Job Board 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /settings/account of the component My Profile Page. The manipulation of the argument filename leads to unrestricted upload. The attack may be launched remotely. The identifier of this vulnerability is VDB-232952. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-3502	A vulnerability, which was classified as critical, was found in SourceCodester Shopping Website 1.0. Affected is an unknown function of the file search-result.php. The manipulation of the argument product leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-232950 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-3458	A vulnerability was found in SourceCodester Shopping Website 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file forgot-password.php. The manipulation of the argument contact 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-232675.	6.3	More Details
CVE-2022-26899	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	6.3	More Details
CVE-2023-27866	IBM Informix JDBC Driver 4.10 and 4.50 is susceptible to remote code execution attack via JNDI injection when driver code or the application using the driver do not verify supplied LDAP URL in Connect String. IBM X-Force ID: 249511.	6.3	More Details
CVE-2023-3457	A vulnerability was found in SourceCodester Shopping Website 1.0. It has been classified as critical. Affected is an unknown function of the file index.php. The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-232674 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-20199	A vulnerability in Cisco Duo Two-Factor Authentication for macOS could allow an authenticated, physical attacker to bypass secondary authentication and access an affected macOS device. This vulnerability is due to the incorrect handling of responses from Cisco Duo when the application is configured to fail open. An attacker with primary user credentials could exploit this vulnerability by attempting to authenticate to an affected device. A successful exploit could allow the attacker to access the affected device without valid permission.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36810	pypdf is a pure-python PDF library capable of splitting, merging, cropping, and transforming the pages of PDF files. An attacker who uses this vulnerability can craft a PDF which leads to unexpected long runtime. This quadratic runtime blocks the current process and can utilize a single core of the CPU by 100%. It does not affect memory usage. This issue has been addressed in PR 808 and versions from 1.27.9 include this fix. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.2	More Details
CVE-2023-22815	Post-authentication remote command injection vulnerability in Western Digital My Cloud OS 5 devices that could allow an attacker to execute code in the context of the root user on vulnerable CGI files. This vulnerability can only be exploited over the network and the attacker must already have admin/root privileges to carry out the exploit. An authentication bypass is required for this exploit, thereby making it more complex. The attack may not require user interaction. Since an attacker must already be authenticated, the confidentiality impact is low while the integrity and availability impact is high. This issue affects My Cloud OS 5 devices: before 5.26.300.	6.2	More Details
CVE-2023-21624	Information disclosure in DSP Services while loading dynamic module.	6.2	More Details
CVE-2023-36807	pypdf is a pure-python PDF library capable of splitting, merging, cropping, and transforming the pages of PDF files. In version 2.10.5 an attacker who uses this vulnerability can craft a PDF which leads to an infinite loop. This infinite loop blocks the current process and can utilize a single core of the CPU by 100%. It does not affect memory usage. That is, for example, the case if the user extracted metadata from such a malformed PDF. Versions prior to 2.10.5 throw an error, but do not hang forever. This issue was fixed with https://github.com/py-pdf/pypdf/pull/1331 which has been included in release 2.10.6. Users are advised to upgrade. Users unable to upgrade should modify `PyPDF2/generic/_data_structures.py::read_object` to an an error throwing case. See GHSA-hm9v-vj3r-r55m for details.	6.2	More Details
CVE-2023-3479	Cross-site Scripting (XSS) - Reflected in GitHub repository hestiacp/hestiacp prior to 1.7.8.	6.1	More Details
CVE-2023-37298	Joplin before 2.11.5 allows XSS via a USE element in an SVG document.	6.1	More Details
CVE-2023-37299	Joplin before 2.11.5 allows XSS via an AREA element of an image map.	6.1	More Details
CVE-2023-28364	An Open Redirect vulnerability exists prior to version 1.52.117, where the built-in QR scanner in Brave Browser Android navigated to scanned URLs automatically without showing the URL first. Now the user must manually navigate to the URL.	6.1	More Details
CVE-2023-34840	angular-ui-notification v0.1.0, v0.2.0, and v0.3.6 was discovered to contain a cross-site scripting (XSS) vulnerability.	6.1	More Details
CVE-2021-34506	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	6.1	More Details
CVE-2023-37302	An issue was discovered in SiteLinksView.php in Wikibase in MediaWiki through 1.39.3. There is XSS via a crafted badge title attribute. This is also related to lack of escaping in wbTemplate (from resources/wikibase/templates.js) for quotes (which can be in a title attribute).	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33276	The web interface of Gira Giersiepen Gira KNX/IP-Router 3.1.3683.0 and 3.3.8.0 responds with a "404 - Not Found" status code if a path is accessed that does not exist. However, the value of the path is reflected in the response. As the application will reflect the supplied path without context-sensitive HTML encoding, it is vulnerable to reflective cross-site scripting (XSS).	6.1	More Details
CVE-2023-20119	A vulnerability in the web-based management interface of Cisco AsyncOS Software for Cisco Secure Email and Web Manager, formerly known as Content Security Management Appliance (SMA) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient user input validation. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	6.1	More Details
CVE-2023-33661	Multiple cross-site scripting (XSS) vulnerabilities were discovered in Church CRM v4.5.3 in GroupReports.php via GroupRole, ReportModel, and OnlyCart parameters.	6.1	More Details
CVE-2023-36816	2FA is a Web app to manage Two-Factor Authentication (2FA) accounts and generate their security codes. Cross site scripting (XSS) injection can be done via the account/service field. This was tested in docker-compose environment. This vulnerability has been patched in version 4.0.3.	6.1	More Details
CVE-2023-3139	The Protect WP Admin WordPress plugin before 4.0 discloses the URL of the admin panel via a redirection of a crafted URL, bypassing the protection offered.	6.1	More Details
CVE-2023-34648	A Cross Site Scripting vulnerability in PHPgurukl User Registration Login and User Management System with admin panel v.1.0 allows a local attacker to execute arbitrary code via a crafted script to the signup.php.	6.1	More Details
CVE-2021-25828	Emby Server versions < 4.6.0.50 is vulnerable to Cross Site Scripting (XSS) vulnerability via a crafted GET request to /web.	6.1	More Details
CVE-2023-34486	itsourcecode Online Hotel Management System Project In PHP v1.0.0 is vulnerable to Cross Site Scripting (XSS). Remote code execution can be achieved by entering malicious code in the date selection box.	6.1	More Details
CVE-2023-2333	The Ninja Forms Google Sheet Connector WordPress plugin before 1.2.7, gsheetconnector-ninja-forms-pro WordPress plugin through 1.2.7 does not escape a parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-34652	PHPgurukl Hostel Management System v.1.0 is vulnerable to Cross Site Scripting (XSS) via Add New Course.	6.1	More Details
CVE-2023-34599	Multiple Cross-Site Scripting (XSS) vulnerabilities have been identified in Gibbon v25.0.0, which enable attackers to execute arbitrary Javascript code.	6.1	More Details
CVE-2023-34650	PHPgurukl Small CRM v.1.0 is vulnerable to Cross Site Scripting (XSS).	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37251	An issue was discovered in the GoogleAnalyticsMetrics extension for MediaWiki through 1.39.3. The googleanalyticstrackurl parser function does not properly escape JavaScript in the onclick handler and does not prevent use of javascript: URLs.	6.1	More Details
CVE-2023-37254	An issue was discovered in the Cargo extension for MediaWiki through 1.39.3. XSS can occur in Special:CargoQuery via a crafted page item when using the default format.	6.1	More Details
CVE-2023-37255	An issue was discovered in the CheckUser extension for MediaWiki through 1.39.3. In Special:CheckUser, a check of the "get edits" type is vulnerable to HTML injection through the User-Agent HTTP request header.	6.1	More Details
CVE-2023-37256	An issue was discovered in the Cargo extension for MediaWiki through 1.39.3. It allows one to store javascript: URLs in URL fields, and automatically links these URLs.	6.1	More Details
CVE-2023-2324	The Elementor Forms Google Sheet Connector WordPress plugin before 1.0.7, gsheetconnector-for-elementor-forms-pro WordPress plugin through 1.0.7 does not escape some parameters before outputting them back in attributes, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-2321	The WPForms Google Sheet Connector WordPress plugin before 3.4.6, gsheetconnector-wpforms-pro WordPress plugin through 3.4.6 does not escape a parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-36484	ILIAS 7.21 and 8.0_beta1 through 8.2 is vulnerable to reflected Cross-Site Scripting (XSS).	6.1	More Details
CVE-2023-36291	Cross Site Scripting vulnerability in Maxsite CMS v.108.7 allows a remote attacker to execute arbitrary code via the f_content parameter in the admin/page_new file.	6.1	More Details
CVE-2023-2320	The CF7 Google Sheets Connector WordPress plugin before 5.0.2, cf7-google-sheets-connector-pro WordPress plugin through 5.0.2 does not escape a parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-34651	PHPgurukl Hospital Management System v.1.0 is vulnerable to Cross Site Scripting (XSS).	6.1	More Details
CVE-2023-34647	PHPgurukl Hostel Management System v.1.0 is vulnerable to Cross Site Scripting (XSS).	6.1	More Details
CVE-2023-21513	Improper privilege management vulnerability in CC Mode prior to SMR Jun-2023 Release 1 allows physical attackers to manipulate device to operate in way that results in unexpected behavior in CC Mode under specific condition.	6.1	More Details
CVE-2023-22816	A post-authentication remote command injection vulnerability in a CGI file in Western Digital My Cloud OS 5 devices that could allow an attacker to build files with redirects and execute larger payloads. This issue affects My Cloud OS 5 devices: before 5.26.300.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37360	pacparser_find_proxy in Pacparser before 1.4.2 allows JavaScript injection, and possibly privilege escalation, when the attacker controls the URL (which may be realistic within enterprise security products).	5.9	More Details
CVE-2023-36610	The affected TBox RTUs generate software security tokens using insufficient entropy. The random seed used to generate the software tokens is not initialized correctly, and other parts of the token are generated using predictable time-based values. An attacker with this knowledge could successfully brute force the token and authenticate themselves.	5.9	More Details
CVE-2023-1206	A hash collision flaw was found in the IPv6 connection lookup table in the Linux kernel's IPv6 functionality when a user makes a new kind of SYN flood attack. A user located in the local network or with a high bandwidth connection can increase the CPU usage of the server that accepts IPV6 connections up to 95%.	5.7	More Details
CVE-2023-21160	In BuildSetTcsFci of protocolmiscbuilder.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-263784118References: N/A	5.5	More Details
CVE-2023-21155	In BuildSetRadioNode of protocolmiscbuilder.cpp, there is a possible out of bounds read due to a missing null check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-264540700References: N/A	5.5	More Details
CVE-2023-21173	In multiple methods of DataUsageList.java, there is a possible way to learn about admin user's network activities due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262741858	5.5	More Details
CVE-2023-21152	In FaceStatsAnalyzer::InterpolateWeightList of face_stats_analyzer.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-269174022References: N/A	5.5	More Details
CVE-2023-21177	In requestAppKeyboardShortcuts of WindowManagerService.java, there is a possible way to infer the app a user is interacting with due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-273906410	5.5	More Details
CVE-2022-48505	This issue was addressed with improved data protection. This issue is fixed in macOS Ventura 13. An app may be able to modify protected parts of the file system	5.5	More Details
CVE-2023-2908	A null pointer dereference issue was found in Libtiff's tif_dir.c file. This issue may allow an attacker to pass a crafted TIFF image file to the tiffcp utility which triggers a runtime error that causes undefined behavior. This will result in an application crash, eventually leading to a denial of service.	5.5	More Details
CVE-2023-21205	In startWpsPinDisplayInternal of sta_iface.cpp, there is a possible out of bounds read due to unsafe deserialization. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262245376	5.5	More Details
CVE-2023-3357	A NULL pointer dereference flaw was found in the Linux kernel AMD Sensor Fusion Hub driver. This flaw allows a local user to crash the system.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3358	A null pointer dereference was found in the Linux kernel's Integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system.	5.5	More Details
CVE-2023-3359	An issue was discovered in the Linux kernel brcm_nvram_parse in drivers/nvmem/brcm_nvram.c. Lacks for the check of the return value of kzalloc() can cause the NULL Pointer Dereference.	5.5	More Details
CVE-2023-3449	A vulnerability has been found in IBOS OA 4.5.5 and classified as critical. This vulnerability affects the function actionExport of the file ?r=recruit/interview/export&interviews=x of the component Interview Management Export. The manipulation of the argument interviews leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-232546 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-21237	In applyRemoteView of NotificationContentInflater.java, there is a possible way to hide foreground service notification due to misleading or insufficient UI. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-251586912	5.5	More Details
CVE-2023-25433	libtiff 4.5.0 is vulnerable to Buffer Overflow via /libtiff/tools/tiffcrop.c:8499. Incorrect updating of buffer size after rotateImage() in tiffcrop cause heap-buffer-overflow and SEGV.	5.5	More Details
CVE-2023-26966	libtiff 4.5.0 is vulnerable to Buffer Overflow in uv_encode() when libtiff reads a corrupted little-endian TIFF file and specifies the output to be big-endian.	5.5	More Details
CVE-2023-29147	In Malwarebytes EDR 1.0.11 for Linux, it is possible to bypass the detection layers that depend on inode identifiers, because an identifier may be reused when a file is replaced, and because two files on different filesystems can have the same identifier.	5.5	More Details
CVE-2023-21211	In multiple files, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262235998	5.5	More Details
CVE-2023-30259	A Buffer Overflow vulnerability in importshp plugin in LibreCAD 2.2.0 allows attackers to obtain sensitive information via a crafted DBF file.	5.5	More Details
CVE-2023-21167	In setProfileName of DevicePolicyManagerService.java, there is a possible way to crash the SystemUI menu due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-259942964	5.5	More Details
CVE-2023-28387	"NewsPicks" App for Android versions 10.4.5 and earlier and "NewsPicks" App for iOS versions 10.4.2 and earlier use hard-coded credentials, which may allow a local attacker to analyze data in the app and to obtain API key for an external service.	5.5	More Details
CVE-2023-21198	In remove_sdp_record of btif_sdp_server.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-245517503	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21168	In convertCbYCrY of ColorConverter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-253270285	5.5	More Details
CVE-2023-21200	In on_remove_iso_data_path of btm_iso_impl.h, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-236688764	5.5	More Details
CVE-2022-4623	The ND Shortcodes WordPress plugin before 7.0 does not validate and escape numerous of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2023-37307	In MISP before 2.4.172, title_for_layout is not properly sanitized in Correlations, CorrelationExclusions, and Layouts.	5.4	More Details
CVE-2023-34831	The "Submission Web Form" of Turnitin LTI tool/plugin version 1.3 is affected by HTML Injection attacks. The security issue affects the submission web form ("id" and "title" HTTP POST parameters) where the students submit their reports for similarity/plagiarism checks.	5.4	More Details
CVE-2023-3331	Improper Limitation of a Pathname to a Restricted Directory vulnerability in NEC Corporation Aterm Aterm WG2600HP2, WG2600HP, WG2200HP, WG1800HP2, WG1800HP, WG1400HP, WG600HP, WG300HP, WF300HP, WR9500N, WR9300N, WR8750N, WR8700N, WR8600N, WR8370N, WR8175N and WR8170N all versions allows a attacker to delete specific files in the product.	5.4	More Details
CVE-2020-22152	Cross Site Scripting vulnerability in daylight studio FUEL- CMS v.1.4.6 allows a remote attacker to execute arbitrary code via the page title, meta description and meta keywords of the pages function.	5.4	More Details
CVE-2021-34475	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	5.4	More Details
CVE-2023-36222	Cross Site Scripting vulnerability in mlogclub bbs-go v. 3.5.5. and before allows a remote attacker to execute arbitrary code via a crafted payload to the comment parameter in the article function.	5.4	More Details
CVE-2023-36223	Cross Site Scripting vulnerability in mlogclub bbs-go v. 3.5.5. and before allows a remote attacker to execute arbitrary code via a crafted payload to the announcements parameter in the settings function.	5.4	More Details
CVE-2023-36488	ILIAS 7.21 and 8.0_beta1 through 8.2 is vulnerable to stored Cross Site Scripting (XSS).	5.4	More Details
CVE-2023-20028	Multiple vulnerabilities in the web-based management interface of Cisco AsyncOS Software for Cisco Secure Email and Web Manager; Cisco Secure Email Gateway, formerly Cisco Email Security Appliance (ESA); and Cisco Secure Web Appliance, formerly Cisco Web Security Appliance (WSA), could allow a remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. For more information about these vulnerabilities, see the Details section of this advisory.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37304	An issue was discovered in the DoubleWiki extension for MediaWiki through 1.39.3. includes/DoubleWiki.php allows XSS via the column alignment feature.	5.4	More Details
CVE-2023-32607	Stored cross-site scripting vulnerability in Pleasanter (Community Edition and Enterprise Edition) 1.3.39.2 and earlier versions allows a remote authenticated attacker to inject an arbitrary script.	5.4	More Details
CVE-2023-20120	Multiple vulnerabilities in the web-based management interface of Cisco AsyncOS Software for Cisco Secure Email and Web Manager; Cisco Secure Email Gateway, formerly Cisco Email Security Appliance (ESA); and Cisco Secure Web Appliance, formerly Cisco Web Security Appliance (WSA), could allow a remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. For more information about these vulnerabilities, see the Details section of this advisory.	5.4	More Details
CVE-2023-3427	The Salon Booking System plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 8.4.6. This is due to missing or incorrect nonce validation on the 'save_customer' function. This makes it possible for unauthenticated attackers to change the admin role to customer or change the user meta to arbitrary values via a forged request, granted they can trick a site administrator into performing an action such as clicking on a link.	5.4	More Details
CVE-2023-36146	A Stored Cross-Site Scripting (XSS) vulnerability was found in Multilaser RE 170 using firmware 2.2.6733.	5.4	More Details
CVE-2023-36617	A ReDoS issue was discovered in the URI component before 0.12.2 for Ruby. The URI parser mishandles invalid URLs that have specific characters. There is an increase in execution time for parsing strings to URI objects with rfc2396_parser.rb and rfc3986_parser.rb. NOTE: this issue exists becuse of an incomplete fix for CVE-2023-28755. Version 0.10.3 is also a fixed version.	5.3	More Details
CVE-2023-36539	Exposure of information intended to be encrypted by some Zoom clients may lead to disclosure of sensitive information.	5.3	More Details
CVE-2023-34834	A Directory Browsing vulnerability in MCL-Net version 4.3.5.8788 webserver running on default port 5080, allows attackers to gain sensitive information about the configured databases via the "/file" endpoint.	5.3	More Details
CVE-2023-37378	Nullsoft Scriptable Install System (NSIS) before 3.09 mishandles access control for an uninstaller directory.	5.3	More Details
CVE-2023-36607	The affected TBox RTUs are missing authorization for running some API commands. An attacker running these commands could reveal sensitive information such as software versions and web server file contents.	5.3	More Details
CVE-2023-37305	An issue was discovered in the ProofreadPage (aka Proofread Page) extension for MediaWiki through 1.39.3. In includes/Page/PageContentHandler.php and includes/Page/PageDisplayHandler.php, hidden users can be exposed via public interfaces.	5.3	More Details
CVE-2023-34658	Telegram v9.6.3 on iOS allows attackers to hide critical information on the User Interface via calling the function SFSafariViewController.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37300	An issue was discovered in the CheckUserLog API in the CheckUser extension for MediaWiki through 1.39.3. There is incorrect access control for visibility of hidden users.	5.3	More Details
CVE-2023-37301	An issue was discovered in SubmitEntityAction in Wikibase in MediaWiki through 1.39.3. Because it doesn't use EditEntity for undo and restore, the intended interaction with AbuseFilter does not occur.	5.3	More Details
CVE-2023-21190	In btm_acl_encrypt_change of btm_acl.cc, there is a possible way for a remote device to turn off encryption without resulting in a terminated connection due to an unusual root cause. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-251436534	5.0	More Details
CVE-2023-33336	Reflected cross site scripting (XSS) vulnerability was discovered in Sophos Web Appliance v4.3.9.1 that allows for arbitrary code to be inputted via the double quotes.	4.8	More Details
CVE-2023-3332	Improper Neutralization of Input During Web Page Generation vulnerability in NEC Corporation Aterm Aterm WG2600HP2, WG2600HP, WG2200HP, WG1800HP2, WG1800HP, WG1400HP, WG600HP, WG300HP, WF300HP, WR9500N, WR9300N, WR8750N, WR8700N, WR8600N, WR8370N, WR8175N and WR8170N all versions allows a attacker to execute an arbitrary script, after obtaining a high privilege exploiting CVE-2023-3330 and CVE-2023-3331 vulnerabilities.	4.8	More Details
CVE-2023-3469	Cross-site Scripting (XSS) - Reflected in GitHub repository thorsten/phpmyfaq prior to 3.2.0-beta.2.	4.8	More Details
CVE-2023-20188	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to view a page containing malicious HTML or script content. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker would need to have valid credentials to access the web-based management interface of the affected device. Cisco has not released software updates to address this vulnerability.	4.8	More Details
CVE-2023-34734	Annet AC Centralized Management Platform 1.02.040 is vulnerable to Stored Cross-Site Scripting (XSS) .	4.8	More Details
CVE-2022-46407	Ericsson Network Manager (ENM), versions prior to 22.2, contains a vulnerability in the REST endpoint “editprofile” where Open Redirect HTTP Header Injection can lead to redirection of the submitted request to domain out of control of ENM deployment. The attacker would need admin/elevated access to exploit the vulnerability	4.8	More Details
CVE-2023-3445	Cross-site Scripting (XSS) - Stored in GitHub repository spinacms/spina prior to 2.15.1.	4.8	More Details
CVE-2023-3034	Reflected XSS affects the ‘mode’ parameter in the /admin functionality of the web application in versions <=2.0.44	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3355	A NULL pointer dereference flaw was found in the Linux kernel's drivers/gpu/drm/msm/msm_gem_submit.c code in the submit_lookup_cmds function, which fails because it lacks a check of the return value of kmalloc(). This issue allows a local user to crash the system.	4.7	More Details
CVE-2023-3478	A vulnerability classified as critical was found in IBOS OA 4.5.5. Affected by this vulnerability is the function actionEdit of the file ?r=dashboard/roleadmin/edit&op=member of the component Add User Handler. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-232759. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2022-23264	Microsoft Edge (Chromium-based) Spoofing Vulnerability	4.7	More Details
CVE-2023-3439	A flaw was found in the MCTP protocol in the Linux kernel. The function mctp_unregister() reclaims the device's relevant resource when a netcard detaches. However, a running routine may be unaware of this and cause the use-after-free of the mdev->addrs object, potentially leading to a denial of service.	4.7	More Details
CVE-2023-3473	A vulnerability, which was classified as critical, was found in Campcodes Retro Cellphone Online Store 1.0. Affected is an unknown function of the file /admin/edit_product.php. The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-232752.	4.7	More Details
CVE-2023-3450	A vulnerability was found in Ruijie RG-BCR860 2.5.13 and classified as critical. This issue affects some unknown processing of the component Network Diagnostic Page. The manipulation leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-232547. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2023-3497	Out of bounds read in Google Security Processor firmware in Google Chrome on Chrome OS prior to 114.0.5735.90 allowed a local attacker to perform denial of service via physical access to the device. (Chromium security severity: Medium)	4.6	More Details
CVE-2023-21202	In btm_delete_stored_link_key_complete of btm_devctl.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure over Bluetooth with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260568359	4.5	More Details
CVE-2023-21195	In btm_ble_periodic_adv_sync_tx_rcvd of btm_ble_gap.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure over Bluetooth, if the firmware were compromised with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-233879420	4.5	More Details
CVE-2023-20758	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636130.	4.4	More Details
CVE-2023-21154	In StoreAdbSerialNumber of protocolmiscbuilder.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-263783910References: N/A	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20759	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07634601.	4.4	More Details
CVE-2023-21181	In btm_ble_update_inq_result of btm_ble_gap.cc, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-264880969	4.4	More Details
CVE-2023-21182	In Exynos_parsing_user_data_registered_itu_t_t35 of VendorVideoAPI.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-252764175	4.4	More Details
CVE-2023-21156	In BuildGetRadioNode of protocolmiscbulider.cpp, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure from the modem with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-264540759References: N/A	4.4	More Details
CVE-2023-21194	In gatt_dbg_op_name of gatt_utils.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260079141	4.4	More Details
CVE-2023-21170	In executeSetClientTarget of ComposerCommandEngine.h, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-252764410	4.4	More Details
CVE-2023-21158	In encode of miscdata.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-263783635References: N/A	4.4	More Details
CVE-2023-21148	In BuildSetConfig of protocolimsbuilder.cpp, there is a possible out of bounds read due to a missing null check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-263783657References: N/A	4.4	More Details
CVE-2023-21196	In btm_ble_batchscan_filter_track_adv_vse_cback of btm_ble_batchscan.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261857395	4.4	More Details
CVE-2023-21199	In btu_ble_proc_ltk_req of btu_hcif.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-254445961	4.4	More Details
CVE-2023-20748	In display, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07536951; Issue ID: ALPS07536951.	4.4	More Details
CVE-2023-21188	In btm_ble_update_inq_result of btm_ble_gap.cc, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-264624283	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21176	In list_key_entries of utils.rs, there is a possible way to disable user credentials due to resource exhaustion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-222287335	4.4	More Details
CVE-2023-21150	In handle_set_parameters_ctrl of hal_socket.c, 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.Product: AndroidVersions: Android kernelAndroid ID: A-267312009References: N/A	4.4	More Details
CVE-2023-21210	In initiateHs20IconQueryInternal of sta_iface.cpp, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262236331	4.4	More Details
CVE-2023-1602	The Short URL plugin for WordPress is vulnerable to stored Cross-Site Scripting via the 'comment' parameter due to insufficient input sanitization and output escaping in versions up to, and including, 1.6.4. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	4.4	More Details
CVE-2023-21204	In multiple files, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the wifi server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262246231	4.4	More Details
CVE-2023-21214	In addGroupWithConfigInternal of p2p_iface.cpp, there is a possible out of bounds read due to unsafe deserialization. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262235736	4.4	More Details
CVE-2023-21213	In initiateTdlsTeardownInternal of sta_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the wifi server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262235951	4.4	More Details
CVE-2023-21212	In multiple files, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the wifi server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262236031	4.4	More Details
CVE-2023-21208	In setCountryCodeInternal of sta_iface.cpp, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262245254	4.4	More Details
CVE-2023-21169	In inviteInternal of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-274443441	4.4	More Details
CVE-2023-3438	An unquoted Windows search path vulnerability existed in the install the MOVE 4.10.x and earlier Windows install service (mvagtsce.exe). The misconfiguration allowed an unauthorized local user to insert arbitrary code into the unquoted service path to obtain privilege escalation and stop antimalware services.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21206	In initiateVenueUrlAnqpQueryInternal of sta_iface.cpp, there is a possible out of bounds read due to unsafe deserialization. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262245630	4.4	More Details
CVE-2023-21518	Improper access control vulnerability in SearchWidget prior to version 3.3 in China models allows untrusted applications to start arbitrary activity.	4.4	More Details
CVE-2020-36741	The MultiVendorX plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.5.7. This is due to missing or incorrect nonce validation on the submit_comment() function. This makes it possible for unauthenticated attackers to submit comments via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2020-36740	The Radio Buttons for Taxonomies plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.0.5. This is due to missing or incorrect nonce validation on the save_single_term() function. This makes it possible for unauthenticated attackers to save terms via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2020-36739	The Feed Them Social – Page, Post, Video, and Photo Galleries plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.8.6. This is due to missing or incorrect nonce validation on the my_fts_fb_load_more() function. This makes it possible for unauthenticated attackers to load feeds via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4387	The Opal Estate plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.6.11. This is due to missing or incorrect nonce validation on the opalestate_set_feature_property() and opalestate_remove_feature_property() functions. This makes it possible for unauthenticated attackers to set and remove featured properties via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-20136	A vulnerability in the OpenAPI of Cisco Secure Workload could allow an authenticated, remote attacker with the privileges of a read-only user to execute operations that should require Administrator privileges. The attacker would need valid user credentials. This vulnerability is due to improper role-based access control (RBAC) of certain OpenAPI operations. An attacker could exploit this vulnerability by issuing a crafted OpenAPI function call with valid credentials. A successful exploit could allow the attacker to execute OpenAPI operations that are reserved for the Administrator user, including the creation and deletion of user labels.	4.3	More Details
CVE-2021-4384	The WordPress Photo Gallery – Image Gallery plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.0.6. This is due to missing or incorrect nonce validation on the load_images_thumbnail() and edit_gallery() functions. This makes it possible for unauthenticated attackers to edit galleries via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-3330	Improper Limitation of a Pathname to a Restricted Directory vulnerability in NEC Corporation Aterm WG2600HP2, WG2600HP, WG2200HP, WG1800HP2, WG1800HP, WG1400HP, WG600HP, WG300HP, WF300HP, WR9500N, WR9300N, WR8750N, WR8700N, WR8600N, WR8370N, WR8175N and WR8170N all versions allows a attacker to obtain specific files in the product.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36738	The Cool Timeline (Horizontal & Vertical Timeline) plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.0.2. This is due to missing or incorrect nonce validation on the ctl_save() function. This makes it possible for unauthenticated attackers to save field icons via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2020-36737	The Import / Export Customizer Settings plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.0.3. This is due to missing or incorrect nonce validation on the astra_admin_errors() function. This makes it possible for unauthenticated attackers to display an import status via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2020-36736	The WooCommerce Checkout & Funnel Builder by CartFlows plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.5.15. This is due to missing or incorrect nonce validation on the export_json, import_json, and status_logs_file functions. This makes it possible for unauthenticated attackers to import/export settings and trigger logs showing via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2020-36735	The WP ERP	Complete HR solution with recruitment & job listings	WooCommerce CRM & Accounting plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.6.3. This is due to missing or incorrect nonce validation on the handle_leave_calendar_filter, add_enable_disable_option_save, leave_policies, process_bulk_action, and process_crm_contact functions. This makes it possible for unauthenticated attackers to modify the plugins settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-42307	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	4.3	More Details
CVE-2023-1844	The Subscribe2 plugin for WordPress is vulnerable to unauthorized access to email functionality due to a missing capability check when sending test emails in versions up to, and including, 10.40. This makes it possible for author-level attackers to send emails with arbitrary content and attachments to site users.	4.3	More Details
CVE-2023-3407	The Subscribe2 plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 10.40. This is due to missing or incorrect nonce validation when sending test emails. This makes it possible for unauthenticated attackers to send test emails with custom content to users on sites running a vulnerable version of this plugin via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-30955	A security defect was identified in Foundry workspace-server that enabled a user to bypass an authorization check and view settings related to 'Developer Mode'. This enabled users with insufficient privilege the ability to view and interact with Developer Mode settings in a limited capacity. A fix was deployed with workspace-server 7.7.0.	4.3	More Details
CVE-2020-36744	The NotificationX plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.8.2. This is due to missing or incorrect nonce validation on the generate_conversions() function. This makes it possible for unauthenticated attackers to generate conversions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4395	The Abandoned Cart Recovery for WooCommerce plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.0.4. This is due to missing or incorrect nonce validation on the get_items() and extra_tablenav() functions. This makes it possible for unauthenticated attackers to perform read-only actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2020-36747	The Lightweight Sidebar Manager plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.4. This is due to missing or incorrect nonce validation on the metabox_save() function. This makes it possible for unauthenticated attackers to save metbox data via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2020-36742	The Custom Field Template plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.5.1. This is due to missing or incorrect nonce validation on the edit_meta_value() function. This makes it possible for unauthenticated attackers to edit meta field values via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4404	The Event Espresso 4 Decaf plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.10.11. This is due to missing or incorrect nonce validation on the ajaxHandler() function. This makes it possible for unauthenticated attackers to op into notifications via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4403	The Remove Schema plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.5. This is due to missing or incorrect nonce validation on the validate() function. This makes it possible for unauthenticated attackers to modify the plugins settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4402	The Multiple Roles plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.3.1. This is due to missing or incorrect nonce validation on the mu_add_roles_in_signup_meta() and mu_add_roles_in_signup_meta_recently() functions. This makes it possible for unauthenticated attackers to add additional roles to users via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4400	The Better Search plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.5.2. This is due to missing or incorrect nonce validation on the bsearch_process_settings_import() and bsearch_process_settings_export() functions. This makes it possible for unauthenticated attackers to import and export settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4399	The Edwiser Bridge plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including,2.0.6. This is due to missing or incorrect nonce validation on the user_data_synchronization_initiater(), course_synchronization_initiater(), users_link_to_moodle_synchronization(), connection_test_initiater(), admin_menus(), and subscribe_handler() function. This makes it possible for unauthenticated attackers to perform unauthorized actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4397	The Staff Directory Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.6. This is due to missing or incorrect nonce validation on the saveCustomFields() function. This makes it possible for unauthenticated attackers to save custom fields via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4396	The Rucy plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 0.4.4. This is due to missing or incorrect nonce validation on the save_rc_post_meta() function. This makes it possible for unauthenticated attackers to save post meta via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2020-36749	The Easy Testimonials plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.6.1. This is due to missing or incorrect nonce validation on the saveCustomFields() function. This makes it possible for unauthenticated attackers to save custom fields via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2020-36748	The Dokan plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.0.8. This is due to missing or incorrect nonce validation on the handle_order_export() function. This makes it possible for unauthenticated attackers to trigger an order export via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4405	The ElasticPress plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.5.3. This is due to missing or incorrect nonce validation on the epio_send_autosuggest_allowed() function. This makes it possible for unauthenticated attackers to send allowed parameters for autosuggest to elasticpress[.]io via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2020-36746	The Menu Swapper plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.0.2. This is due to missing or incorrect nonce validation on the mswp_save_meta() function. This makes it possible for unauthenticated attackers to save meta data via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4391	The Ultimate Gift Cards for WooCommerce plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.1.1. This is due to missing or incorrect nonce validation on the mwb_wgm_save_post() function. This makes it possible for unauthenticated attackers to modify product gift card details via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2020-36743	The Product Catalog Simple plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.5.13. This is due to missing or incorrect nonce validation on the implecode_save_products_meta() function. This makes it possible for unauthenticated attackers to update product meta via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2020-36745	The WP Project Manager plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.4.0. This is due to missing or incorrect nonce validation on the do_updates() function. This makes it possible for unauthenticated attackers to trigger updates via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4389	The WP Travel plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.4.6. This is due to missing or incorrect nonce validation on the save_meta_data() function. This makes it possible for unauthenticated attackers to save metadata for travel posts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4390	The Contact Form 7 Style plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.2. This is due to missing or incorrect nonce validation on the manage_wp_posts_be_qe_save_post() function. This makes it possible for unauthenticated attackers to quick edit templates via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4388	The Opal Estate plugin for WordPress is vulnerable to featured property modifications in versions up to, and including, 1.6.11. This is due to missing capability checks on the opalestate_set_feature_property() and opalestate_remove_feature_property() functions. This makes it possible for unauthenticated attackers to set and remove featured properties.	4.3	More Details
CVE-2021-4392	The eCommerce Product Catalog Plugin for WordPress plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.9.43. This is due to missing or incorrect nonce validation on the implecode_save_products_meta() function. This makes it possible for unauthenticated attackers to save product meta data via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4393	The eCommerce Product Catalog Plugin for WordPress plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.0.17. This is due to missing or incorrect nonce validation on the save() function. This makes it possible for unauthenticated attackers to save manual digital orders via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-35938	Tuleap is a Free & Open Source Suite to improve management of software developments and collaboration. When switching from a project visibility that allows restricted users to `Private without restricted`, restricted users that are project administrators keep this access right. Restricted users that were project administrators before the visibility switch keep the possibility to access the project and do some administration actions. This issue has been resolved in Tuleap version 14.9.99.63. Users are advised to upgrade. There are no known workarounds for this issue.	4.1	More Details
CVE-2023-21178	In installKey of KeyUtil.cpp, there is a possible failure of file encryption due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-140762419	4.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34450	CometBFT is a Byzantine Fault Tolerant (BFT) middleware that takes a state transition machine and replicates it on many machines. An internal modification made in versions 0.34.28 and 0.37.1 to the way struct `PeerState` is serialized to JSON introduced a deadlock when new function MarshallJSON is called. This function can be called from two places. The first is via logs, setting the `consensus` logging module to "debug" level (should not happen in production), and setting the log output format to JSON. The second is via RPC `dump_consensus_state`. Case 1, which should not be hit in production, will eventually hit the deadlock in most goroutines, effectively halting the node. In case 2, only the data structures related to the first peer will be deadlocked, together with the thread(s) dealing with the RPC request(s). This means that only one of the channels of communication to the node's peers will be blocked. Eventually the peer will timeout and excluded from the list (typically after 2 minutes). The goroutines involved in the deadlock will not be garbage collected, but they will not interfere with the system after the peer is excluded. The theoretical worst case for case 2, is a network with only two validator nodes. In this case, each of the nodes only has one `PeerState` struct. If `dump_consensus_state` is called in either node (or both), the chain will halt until the peer connections time out, after which the nodes will reconnect (with different `PeerState` structs) and the chain will progress again. Then, the same process can be repeated. As the number of nodes in a network increases, and thus, the number of peer struct each node maintains, the possibility of reproducing the perturbation visible with two nodes decreases. Only the first `PeerState` struct will deadlock, and not the others (RPC `dump_consensus_state` accesses them in a for loop, so the deadlock at the first iteration causes the rest of the iterations of that "for" loop to never be reached). This regression was fixed in versions 0.34.29 and 0.37.2. Some workarounds are available. For case 1 (hitting the deadlock via logs), either don't set the log output to "json", leave at "plain", or don't set the consensus logging module to "debug", leave it at "info" or higher. For case 2 (hitting the deadlock via RPC `dump_consensus_state`), do not expose `dump_consensus_state` RPC endpoint to the public internet (e.g., via rules in one's nginx setup).	3.7	More Details
CVE-2023-30946	A security defect was identified in Foundry Issues. If a user was added to an issue on a resource that they did not have access to and consequently could not see, they could query Foundry's Notification API and receive metadata about the issue including the RID of the issue, severity, internal UUID of the author, and the user-defined title of the issue.	3.5	More Details
CVE-2023-3465	A vulnerability was found in SimplePHPscripts Classified Ads Script 1.8. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file user.php of the component HTTP POST Request Handler. The manipulation of the argument title leads to cross site scripting. The attack can be launched remotely. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-232711.	3.5	More Details
CVE-2023-3505	A vulnerability was found in Onest CRM 1.0. It has been classified as problematic. This affects an unknown part of the file /admin/project/update/2 of the component Project List Handler. The manipulation of the argument name with the input <script>alert(1)</script> leads to cross site scripting. It is possible to initiate the attack remotely. The identifier VDB-232953 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3506	A vulnerability was found in Active It Zone Active eCommerce CMS 6.5.0. It has been declared as problematic. This vulnerability affects unknown code of the file /ecommerce/support_ticket of the component Create Ticket Page. The manipulation of the argument details with the input <script>alert(1)</script> leads to cross site scripting. The attack can be initiated remotely. VDB-232954 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3464	A vulnerability was found in SimplePHPscripts Classified Ads Script 1.8. It has been classified as problematic. Affected is an unknown function of the file /preview.php of the component URL Parameter Handler. The manipulation of the argument p leads to cross site scripting. It is possible to launch the attack remotely. It is recommended to upgrade the affected component. VDB-232710 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-3477	A vulnerability was found in RocketSoft Rocket LMS 1.7. It has been declared as problematic. This vulnerability affects unknown code of the file /contact/store of the component Contact Form. The manipulation of the argument name/subject/message leads to cross site scripting. The attack can be initiated remotely. The identifier of this vulnerability is VDB-232756.	3.5	More Details
CVE-2023-3475	A vulnerability was found in SimplePHPscripts Event Script 2.1 and classified as problematic. Affected by this issue is some unknown functionality of the file preview.php of the component URL Parameter Handler. The manipulation leads to cross site scripting. The attack may be launched remotely. It is recommended to upgrade the affected component. VDB-232754 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-3474	A vulnerability has been found in SimplePHPscripts Simple Blog 3.2 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file preview.php of the component URL Parameter Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. It is recommended to upgrade the affected component. The identifier VDB-232753 was assigned to this vulnerability.	3.5	More Details
CVE-2023-3476	A vulnerability was found in SimplePHPscripts GuestBook Script 2.2. It has been classified as problematic. This affects an unknown part of the file preview.php of the component URL Parameter Handler. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-232755.	3.5	More Details
CVE-2023-25523	NVIDIA CUDA toolkit for Linux and Windows contains a vulnerability in the nvdisasm binary file, where an attacker may cause a NULL pointer dereference by providing a user with a malformed ELF file. A successful exploit of this vulnerability may lead to a partial denial of service.	3.3	More Details
CVE-2022-29147	Microsoft Edge (Chromium-based) Spoofing Vulnerability	3.1	More Details
CVE-2023-2010	The Forminator WordPress plugin before 1.24.1 does not use an atomic operation to check whether a user has already voted, and then update that information. This leads to a Race Condition that may allow a single user to vote multiple times on a poll.	3.1	More Details
CVE-2023-3485	Insecure defaults in open-source Temporal Server before version 1.20 on all platforms allows an attacker to craft a task token with access to a namespace other than the one specified in the request. Creation of this task token must be done outside of the normal Temporal server flow. It requires the namespace UUID and information from the workflow history for the target namespace. Under these conditions, it is possible to interfere with pending tasks in other namespaces, such as marking a task failed or completed. If a task is targeted for completion by the attacker, the targeted namespace must also be using the same data converter configuration as the initial, valid, namespace for the task completion payload to be decoded by workers in the target namespace.	3.0	More Details
CVE-2023-21512	Improper Knox ID validation logic in notification framework prior to SMR Jun-2023 Release 1 allows local attackers to read work profile notifications without proper access permission.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22507	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-3117	Rejected reason: Duplicate of CVE-2023-3390.	N/A	More Details
CVE-2022-42337	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-36262	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-2022-42338	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-43583	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-43584	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-43585	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-43586	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-43587	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-3370	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-4854	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-34211	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-35073	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35935	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-31999. Reason: This candidate is a reservation duplicate of CVE-2023-31999. Notes: All CVE users should reference CVE-2023-31999 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-35700	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-35999	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-15730	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-36001	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-2570	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details