SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 26 April 2023

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-2131	Versions of INEA ME RTU firmware prior to 3.36 are vulnerable to OS command injection, which could allow an attacker to remotely execute arbitrary code.	10.0	More Details
CVE-2021-33970	Buffer Overflow vulnerability in Qihoo 360 Chrome v13.0.2170.0 allows attacker to escalate priveleges.	10.0	More Details
CVE-2021-33975	Buffer Overflow vulnerability in Qihoo 360 Total Security v10.8.0.1060 and v10.8.0.1213 allows attacker to escalate privileges.	10.0	More Details
CVE-2021-33972	Buffer Overflow vulnerability in Qihoo 360 Safe Browser v13.0.2170.0 allows attacker to escalate priveleges.	10.0	More Details
CVE-2023-30839	PrestaShop is an Open Source e-commerce web application. Versions prior to 8.0.4 and 1.7.8.9 contain a SQL filtering vulnerability. A BO user can write, update, and delete in the database, even without having specific rights. PrestaShop 8.0.4 and 1.7.8.9 contain a patch for this issue. There are no known workarounds.	9.9	More Details
CVE-2023-29524	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. It's possible to execute anything with the right of the Scheduler Application sheet page. A user without script or programming rights, edit your user profile with the object editor and add a new object of type XWiki.SchedulerJobClass, In "Job Script", groovy code can be added and will be executed in the server context on viewing. This has been patched in XWiki 14.10.3 and 15.0 RC1. Users are advised to upgrade. There are no known workarounds for this issue.	9.9	More Details
CVE-2023-29510	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In XWiki, every user can add translations that are only applied to the current user. This also allows overriding existing translations. Such translations are often included in privileged contexts without any escaping which allows remote code execution for any user who has edit access on at least one document which could be the user's own profile where edit access is enabled by default. A mitigation for this vulnerability is part of XWiki 14.10.2 and XWiki 15.0 RC1: translations with user scope now require script right. This means that regular users cannot exploit this anymore as users don't have script right by default anymore starting with XWiki 14.10. There are no known workarounds apart from upgrading to a patched versions.	9.9	More Details
CVE-2023-29526	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions it's possible to display or interact with any page a user cannot access through the combination of the async and display macros. A comment with either macro will be executed when viewed providing a code injection vector in the context of the running server. This vulnerability has been patched in XWiki 15.0-rc-1, 14.10.3, 14.4.8, and 13.10.11. Users are advised to upgrade. There are no known workarounds for this issue.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29525	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Affected versions of xwiki are subject to code injection in the `since` parameter of the `/xwiki/bin/view/XWiki/Notifications/Code/LegacyNotificationAdministration` endpoint. This provides an XWiki syntax injection attack via the since-parameter, allowing privilege escalation from view to programming rights and subsequent code execution privilege. The vulnerability has been patched in XWiki 15.0-rc-1, 14.10.3, 14.4.8 and 14.10.3. Users are advised to upgrade. Users unable to upgrade may modify the page `XWiki.Notifications.Code.LegacyNotificationAdministration` to add the missing escaping. For versions < 14.6-rc-1 a workaround is to modify the file `<xwikiwebapp>/templates/distribution/eventmigration.wiki` to add the missing escaping.	9.9	More Details
CVE-2023-29527	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions a user without script or programming right may edit a user profile (or any other document) with the wiki editor and add groovy script content. Viewing the document after saving it will execute the groovy script in the server context which provides code execution. This vulnerability has been patched in XWiki 15.0-rc-1 and 14.10.3. Users are advised to upgrade. There are no known workarounds for this issue.	9.9	More Details
CVE-2023-29523	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 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. The same vulnerability can also be exploited in other contexts where the `display` method on a document is used to display a field with wiki syntax, for example in applications created using `App Within Minutes`. This has been patched in XWiki 13.10.11, 14.4.8, 14.10.2 and 15.0RC1. There is no workaround apart from upgrading.	9.9	More Details
CVE-2023-29522	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with view rights 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. The attack works by opening a non-existing page with a name crafted to contain a dangerous payload. This issue has been patched in XWiki 14.4.8, 14.10.3 and 15.0RC1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.9	More Details
CVE-2023-29518	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with view rights can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of `Invitation.InvitationCommon`. This page is installed by default. The vulnerability has been patched in XWiki 15.0-rc-1, 14.10.1, 14.4.8, and 13.10.11. Users are advised to upgrade. There are no known workarounds for this issue.	9.9	More Details
CVE-2023-29516	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with view rights on `XWiki.AttachmentSelector` can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping in the "Cancel and return to page" button. This page is installed by default. This vulnerability has been patched in XWiki 15.0-rc-1, 14.10.1, 14.4.8, and 13.10.11. There are no known workarounds for this vulnerability.	9.9	More Details
CVE-2023-29514	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with edit rights on any document (e.g., their own user profile) can execute code with programming rights, leading to remote code execution. This vulnerability has been patched in XWiki 13.10.11, 14.4.8, 14.10.1 and 15.0 RC1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.9	More Details
CVE-2023-29512	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with edit rights on a page (e.g., it's own user page), can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the information loaded from attachments in `imported.vm`, `importinline.vm`, and `packagelist.vm`. This page is installed by default. This vulnerability has been patched in XWiki 15.0-rc-1, 14.10.1, 14.4.8, and 13.10.11. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.9	More Details
CVE-2023-30376	In Tenda AC15 V15.03.05.19, the function "henan_pppoe_user" contains a stack-based buffer overflow vulnerability.	9.8	More Details
CVE-2023-30369	Tenda AC15 V15.03.05.19 is vulnerable to Buffer Overflow.	9.8	More Details
CVE-2023-24819	RIOT-OS, an operating system that supports Internet of Things devices, contains a network stack with the ability to process 6LoWPAN frames. Prior to version 2022.10, an attacker can send a crafted frame to the device resulting in an out of bounds write in the packet buffer. The overflow can be used to corrupt other packets and the allocator metadata. Corrupting a pointer will easily lead to denial of service. While carefully manipulating the allocator metadata gives an attacker the possibility to write data to arbitrary locations and thus execute arbitrary code. Version 2022.10 fixes this issue. As a workaround, disable support for fragmented IP datagrams or apply the patches manually.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30368	Tenda AC5 V15.03.06.28 is vulnerable to Buffer Overflow via the initWebs function.	9.8	More Details
CVE-2023-30370	In Tenda AC15 V15.03.05.19, the function GetValue contains a stack-based buffer overflow vulnerability.	9.8	More Details
CVE-2023-30371	In Tenda AC15 V15.03.05.19, the function "sub_ED14" contains a stack-based buffer overflow vulnerability.	9.8	More Details
CVE-2023-30372	In Tenda AC15 V15.03.05.19, The function "xkjs_ver32" contains a stack-based buffer overflow vulnerability.	9.8	More Details
CVE-2023-30373	In Tenda AC15 V15.03.05.19, the function "xian_pppoe_user" contains a stack-based buffer overflow vulnerability.	9.8	More Details
CVE-2023-30375	In Tenda AC15 V15.03.05.19, the function "getIfIp" contains a stack-based buffer overflow vulnerability.	9.8	More Details
CVE-2023-1020	The Steveas WP Live Chat Shoutbox WordPress plugin through 1.4.2 does not sanitise and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection.	9.8	More Details
CVE-2023-30378	In Tenda AC15 V15.03.05.19, the function "sub_8EE8" contains a stack-based buffer overflow vulnerability.	9.8	More Details
CVE-2023-24823	RIOT-OS, an operating system that supports Internet of Things devices, contains a network stack with the ability to process 6LoWPAN frames. Prior to version 2022.10, an attacker can send a crafted frame to the device resulting in a type confusion between IPv6 extension headers and a UDP header. This occurs while encoding a 6LoWPAN IPHC header. The type confusion manifests in an out of bounds write in the packet buffer. The overflow can be used to corrupt other packets and the allocator metadata. Corrupting a pointer will easily lead to denial of service. While carefully manipulating the allocator metadata gives an attacker the possibility to write data to arbitrary locations and thus execute arbitrary code. Version 2022.10 fixes this issue. As a workaround, apply the patches manually.	9.8	More Details
CVE-2023-26865	SQL injection vulnerability found in PrestaShop bdroppy v.2.2.12 and before allowing a remote attacker to gain privileges via the BdroppyCronModuleFrontController::importProducts component.	9.8	More Details
CVE-2023-27848	broccoli-compass v0.2.4 was discovered to contain a remote code execution (RCE) vulnerability via the child_process function.	9.8	More Details
CVE-2023-27849	rails-routes-to-json v1.0.0 was discovered to contain a remote code execution (RCE) vulnerability via the child_process function.	9.8	More Details
CVE-2023-29566	huedawn-tesseract 0.3.3 and dawnsparks-node-tesseract 0.4.0 to 0.4.1 was discovered to contain a remote code execution (RCE) vulnerability via the child_process function.	9.8	More Details
CVE-2023-22577	Within White Rabbit Switch it's possible as an unauthenticated user to retrieve sensitive information such as password hashes and the SNMP community strings.	9.8	More Details
CVE-2023-28771	Improper error message handling in Zyxel ZyWALL/USG series firmware versions 4.60 through 4.73, VPN series firmware versions 4.60 through 5.35, USG FLEX series firmware versions 4.60 through 5.35, and ATP series firmware versions 4.60 through 5.35, which could allow an unauthenticated attacker to execute some OS commands remotely by sending crafted packets to an affected device.	9.8	More Details
CVE-2023-27105	A vulnerability in the Wi-Fi file transfer module of Shanling M5S Portable Music Player with Shanling MTouch OS v4.3 and Shanling M2X Portable Music Player with Shanling MTouch OS v3.3 allows attackers to arbitrarily read, delete, or modify any critical system files via directory traversal.	9.8	More Details
CVE-2023-25313	OS injection vulnerability in World Wide Broadcast Network AVideo version before 12.4, allows attackers to execute arbitrary code via the video link field to the Embed a video link feature.	9.8	More Details
CVE-2023-22581	White Rabbit Switch contains a vulnerability which makes it possible for an attacker to perform system commands under the context of the web application (the default installation makes the webserver run as the root user).	9.8	More Details
CVE-2021-28254	A deserialization vulnerability in the destruct() function of Laravel v8.5.9 allows attackers to execute arbitrary commands.	9.8	More Details
CVE-2023-20864	VMware Aria Operations for Logs contains a deserialization vulnerability. An unauthenticated, malicious actor with network access to VMware Aria Operations for Logs may be able to execute arbitrary code as root.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20873	In Spring Boot versions 3.0.0 - 3.0.5, 2.7.0 - 2.7.10, and older unsupported versions, an application that is deployed to Cloud Foundry could be susceptible to a security bypass. Users of affected versions should apply the following mitigation: 3.0.x users should upgrade to 3.0.6+. 2.7.x users should upgrade to 2.7.11+. Users of older, unsupported versions should upgrade to 3.0.6+ or 2.7.11+.	9.8	More Details
CVE-2023-21096	In OnWakelockReleased of attribution_processor.cc, there is a use after free that could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-254774758	9.8	More Details
CVE-2023-23451	The Flexi Classic and Flexi Soft Gateways SICK UE410-EN3 FLEXI ETHERNET GATEW. with serial number <=2311xxxx all Firmware versions, SICK UE410-EN1 FLEXI ETHERNET GATEW. with serial number <=2311xxxx all Firmware versions, SICK UE410-EN3S04 FLEXI ETHERNET GATEW. with serial number <=2311xxxx all Firmware versions, SICK UE410-EN4 FLEXI ETHERNET GATEW. with serial number <=2311xxxx all Firmware versions, SICK FX0-GENT00000 FLEXISOFT EIP GATEW. with serial number <=2311xxxx with Firmware <=V2.11.0, SICK FX0-GMOD00000 FLEXISOFT MOD GATEW. with serial number <=2311xxxx with Firmware <=V2.11.0, SICK FX0-GPNT00000 FLEXISOFT PNET GATEW. with serial number <=2311xxxx with Firmware <=V2.12.0, SICK FX0-GENT00030 FLEXISOFT EIP GATEW.V2 with serial number <=2311xxxx all Firmware versions, SICK FX0-GPNT00030 FLEXISOFT PNET GATEW.V2 with serial number <=2311xxxx all Firmware versions and SICK FX0-GMOD00010 FLEXISOFT MOD GW with serial number <=2311xxxx with Firmware <=V2.11.0 all have Telnet enabled by factory default. No password is set in the default configuration.	9.8	More Details
CVE-2022-29604	An issue was discovered in ONOS 2.5.1. An intent with an uppercase letter in a device ID shows the CORRUPT state, which is misleading to a network operator. Improper handling of case sensitivity causes inconsistency between intent and flow rules in the network.	9.8	More Details
CVE-2022-29606	An issue was discovered in ONOS 2.5.1. An intent with a large port number shows the CORRUPT state, which is misleading to a network operator. Improper handling of such port numbers causes inconsistency between intent and flow rules in the network.	9.8	More Details
CVE-2023-29926	PowerJob V4.3.2 has unauthorized interface that causes remote code execution.	9.8	More Details
CVE-2023-27350	This vulnerability allows remote attackers to bypass authentication on affected installations of PaperCut NG 22.0.5 (Build 63914). Authentication is not required to exploit this vulnerability. The specific flaw exists within the SetupCompleted class. The issue results from improper access control. An attacker can leverage this vulnerability to bypass authentication and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-18987.	9.8	More Details
CVE-2023-30076	Sourcecodester Judging Management System v1.0 is vulnerable to SQL Injection via /php-jms/print_judges.php?print_judges.php=&se_name=&sub_event_id=.	9.8	More Details
CVE-2023-31060	Repetier Server through 1.4.10 executes as SYSTEM. This can be leveraged in conjunction with CVE-2023-31059 for full compromise.	9.8	More Details
CVE-2023-29924	PowerJob V4.3.1 is vulnerable to Incorrect Access Control that allows for remote code execution.	9.8	More Details
CVE-2023-2231	A vulnerability, which was classified as critical, was found in MAXTECH MAX-G866ac 0.4.1_TBRO_20160314. This affects an unknown part of the component Remote Management. The manipulation leads to missing authentication. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-227001 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2023-30621	Gipsy is a multi-purpose discord bot which aim to be as modular and user-friendly as possible. In versions prior to 1.3 users can run command on the host machine with sudoer permission. The `!ping` command when provided with an IP or hostname used to run a bash `ping <IP>` without verification that the IP or hostname was legitimate. This command was executed with root permissions and may lead to arbitrary command injection on the host server. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.8	More Details
CVE-2023-23753	The 'Visforms Base Package for Joomla 3' extension is vulnerable to SQL Injection as concatenation is used to construct an SQL Query. An attacker can interact with the database and could be able to read, modify and delete data on it.	9.8	More Details
CVE-2023-1892	Cross-site Scripting (XSS) - Reflected in GitHub repository sidekiq/sidekiq prior to 7.0.8.	9.6	More Details
CVE-2023-2136	Integer overflow in Skia in Google Chrome prior to 112.0.5615.137 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28131	A vulnerability in the expo.io framework allows an attacker to take over accounts and steal credentials on an application/website that configured the "Expo AuthSession Redirect Proxy" for social sign-in. This can be achieved once a victim clicks a malicious link. The link itself may be sent to the victim in various ways (including email, text message, an attacker-controlled website, etc).	9.6	More Details
CVE-2023-25131	Use of default password vulnerability in PowerPanel Business Local/Remote for Windows v4.8.6 and earlier, PowerPanel Business Management for Windows v4.8.6 and earlier, PowerPanel Business Local/Remote for Linux 32bit v4.8.6 and earlier, PowerPanel Business Local/Remote for Linux 64bit v4.8.6 and earlier, PowerPanel Business Management for Linux 32bit v4.8.6 and earlier, PowerPanel Business Management for Linux 64bit v4.8.6 and earlier, PowerPanel Business Local/Remote for MacOS v4.8.6 and earlier, and PowerPanel Business Management for MacOS v4.8.6 and earlier allows remote attackers to log in to the server directly to perform administrative functions. Upon installation or upon first login, the application does not ask the user to change the 'admin' password.	9.4	More Details
CVE-2023-2227	Improper Authorization in GitHub repository modoboa/modoboa prior to 2.1.0.	9.1	More Details
CVE-2023-26556	io.finnet tss-lib before 2.0.0 can leak a secret key via a timing side-channel attack because it relies on the scalar-multiplication implementation in Go crypto/elliptic, which is not constant time (there is an if statement in a loop). One leak is in ecdsa/keygen/round_2.go. (bnb-chain/tss-lib and thorchain/tss are also affected.)	9.1	More Details
CVE-2023-31056	CloverDX before 5.17.3 writes passwords to the audit log in certain situations, if the audit log is enabled and single sign-on is not employed. The fixed versions are 5.15.4, 5.16.2, 5.17.3, and 6.0.x.	9.1	More Details
CVE-2023-25133	Improper privilege management vulnerability in default.cmd file in PowerPanel Business Local/Remote for Windows v4.8.6 and earlier, PowerPanel Business Management for Windows v4.8.6 and earlier, PowerPanel Business Local/Remote for Linux 32bit v4.8.6 and earlier, PowerPanel Business Local/Remote for Linux 64bit v4.8.6 and earlier, PowerPanel Business Management for Linux 32bit v4.8.6 and earlier, PowerPanel Business Management for Linux 64bit v4.8.6 and earlier, PowerPanel Business Local/Remote for MacOS v4.8.6 and earlier, and PowerPanel Business Management for MacOS v4.8.6 and earlier allows remote attackers to execute operation system commands via unspecified vectors.	9.1	More Details
CVE-2023-25132	Unrestricted upload of file with dangerous type vulnerability in default.cmd file in PowerPanel Business Local/Remote for Windows v4.8.6 and earlier, PowerPanel Business Management for Windows v4.8.6 and earlier, PowerPanel Business Local/Remote for Linux 32bit v4.8.6 and earlier, PowerPanel Business Local/Remote for Linux 64bit v4.8.6 and earlier, PowerPanel Business Management for Linux 32bit v4.8.6 and earlier, PowerPanel Business Management for Linux 64bit v4.8.6 and earlier, PowerPanel Business Local/Remote for MacOS v4.8.6 and earlier, and PowerPanel Business Management for MacOS v4.8.6 and earlier allows remote attackers to execute operation system commands via unspecified vectors.	9.1	More Details
CVE-2021-44547	A sandboxing issue in Odoo Community 15.0 and Odoo Enterprise 15.0 allows authenticated administrators to executed arbitrary code, leading to privilege escalation.	9.1	More Details
CVE-2023-29528	XWiki Commons are technical libraries common to several other top level XWiki projects. The "restricted" mode of the HTML cleaner in XWiki, introduced in version 4.2-milestone-1 and massively improved in version 14.6-rc-1, allowed the injection of arbitrary HTML code and thus cross-site scripting via invalid HTML comments. As a consequence, any code relying on this "restricted" mode for security is vulnerable to JavaScript injection ("cross-site scripting"/XSS). When a privileged user with programming rights visits such a comment in XWiki, the malicious JavaScript code is executed in the context of the user session. This allows server-side code execution with programming rights, impacting the confidentiality, integrity and availability of the XWiki instance. This problem has been patched in XWiki 14.10, HTML comments are now removed in restricted mode and a check has been introduced that ensures that comments don't start with `>`. There are no known workarounds apart from upgrading to a version including the fix.	9.0	More Details
CVE-2023-30627	jellyfin-web is the web client for Jellyfin, a free-software media system. Starting in version 10.1.0 and prior to version 10.8.10, a stored cross-site scripting vulnerability in device.js can be used to make arbitrary calls to the `REST` endpoints with admin privileges. When combined with CVE-2023-30626, this results in remote code execution on the Jellyfin instance in the context of the user who's running it. This issue is patched in version 10.8.10. There are no known workarounds.	9.0	More Details
CVE-2023-29519	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. A registered user can perform remote code execution leading to privilege escalation by injecting the proper code in the "property" field of an attachment selector, as a gadget of their own dashboard. Note that the vulnerability does not impact comments of a wiki. The vulnerability has been patched in XWiki 13.10.11, 14.4.8, 14.10.2, 15.0-rc-1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-27524	Session Validation attacks in Apache Superset versions up to and including 2.0.1. Installations that have not altered the default configured SECRET_KEY according to installation instructions allow for an attacker to authenticate and access unauthorized resources. This does not affect Superset administrators who have changed the default value for SECRET_KEY config. All superset installations should always set a unique secure random SECRET_KEY. Your SECRET_KEY is used to securely sign all session cookies and encrypting sensitive information on the database. Add a strong SECRET_KEY to your `superset_config.py` file like: SECRET_KEY = <YOUR_OWN_RANDOM_GENERATED_SECRET_KEY> Alternatively you can set it with `SUPERSET_SECRET_KEY` environment variable.	8.9	More Details
CVE-2021-33974	Qihoo 360 (https://www.360.cn/) Qihoo 360 Safeguard (https://www.360.cn/) Qihoo 360 Chrome (https://browser.360.cn/ee/) is affected by: Buffer Overflow. The impact is: execute arbitrary code (remote). The component is: This is a set of vulnerabilities affecting popular software, and the installation packages correspond to versions "360 Safeguard(12.1.0.1004,12.1.0.1005,13.1.0.1001)" , "360 Total Security(10.8.0.1060,10.8.0.1213)", "360 Safe Browser & 360 Chrome(12. The attack vector is: On the browser vulnerability, just open a link to complete the vulnerability exploitation remotely; on the client software, you need to locally execute the vulnerability exploitation program, which of course can be achieved with the full chain of browser vulnerability. ¶¶ This is a set of the most serious vulnerabilities that exist on Qihoo 360's PC client multiple popular software, remote vulnerabilities can be accomplished by opening a link to arbitrary code execution on both security browsers, in conjunction with the exploitation of local vulnerabilities that allow spyware to persist without being scanned to permanently reside on the target PC computer (because local vulnerabilities target Qihoo 360 company's antivirus software kernel flaws); this set of remote and local vulnerabilities in perfect coordination, to achieve an information security fallacy, on Qihoo 360's antivirus software vulnerability, not only can not be scanned out of the virus, but will help the virus persistently control the target computer, while Qihoo 360 claims to be a secure browser, which exists in the kernel vulnerability but help the composition of the remote vulnerability.(Security expert "Memory Corruptor" have reported this set of vulnerabilities to the corresponding vendor, all vulnerabilities have been fixed and the vendor rewarded thousands of dollars to this security expert)	8.8	More Details
CVE-2023-2137	Heap buffer overflow in sqlite in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-2258	Improper Neutralization of Formula Elements in a CSV File in GitHub repository alfio-event/alf.io prior to 2.0-M4-2304.	8.8	More Details
CVE-2023-2260	Authorization Bypass Through User-Controlled Key in GitHub repository alfio-event/alf.io prior to 2.0-M4-2304.	8.8	More Details
CVE-2023-30626	Jellyfin is a free-software media system. Versions starting with 10.8.0 and prior to 10.8.10 and prior have a directory traversal vulnerability inside the `ClientLogController`, specifically `/ClientLog/Document`. When combined with a cross-site scripting vulnerability (CVE-2023-30627), this can result in file write and arbitrary code execution. Version 10.8.10 has a patch for this issue. There are no known workarounds.	8.8	More Details
CVE-2023-30623	`embano1/wip` is a GitHub Action written in Bash. Prior to version 2, the `embano1/wip` action uses the `github.event.pull_request.title` parameter in an insecure way. The title parameter is used in a run statement - resulting in a command injection vulnerability due to string interpolation. This vulnerability can be triggered by any user on GitHub. They just need to create a pull request with a commit message containing an exploit. (Note that first-time PR requests will not be run - but the attacker can submit a valid PR before submitting an invalid PR). The commit can be genuine, but the commit message can be malicious. This can be used to execute code on the GitHub runners and can be used to exfiltrate any secrets used in the CI pipeline, including repository tokens. Version 2 has a fix for this issue.	8.8	More Details
CVE-2023-30628	Kiwi TCMS is an open source test management system. In kiwitcms/Kiwi v12.2 and prior and kiwitcms/enterprise v12.2 and prior, the `changelog.yml` workflow is vulnerable to command injection attacks because of using an untrusted `github.head_ref` field. The `github.head_ref` value is an attacker-controlled value. Assigning the value to `zzz";echo${IFS}"hello";#` can lead to command injection. Since the permission is not restricted, the attacker has a write-access to the repository. Commit 834c86dfd1b2492ccad7ebbfd6304bfec895fed2 of the kiwitcms/Kiwi repository and commit e39f7e156fdaf6fec09a15ea6f4e8fec8cdbf751 of the kiwitcms/enterprise repository contain a fix for this issue.	8.8	More Details
CVE-2023-25760	Incorrect Access Control in Tripleplay Platform releases prior to Caveman 3.4.0 allows authenticated user to modify other users passwords via a crafted request payload	8.8	More Details
CVE-2022-46302	Broad access controls could allow site users to directly interact with the system Apache installation when providing the reverse proxy configurations for Tribe29's Checkmk <= 2.1.0p6, Checkmk <= 2.0.0p27, and all versions of Checkmk 1.6.0 (EOL) allowing an attacker to perform remote code execution with root privileges on the underlying host.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29849	Bang Resto 1.0 was discovered to contain multiple SQL injection vulnerabilities via the btnMenuItemID, itemID, itemPrice, menuID, staffID, or itemqty parameter.	8.8	More Details
CVE-2023-21085	In nci_snd_set_routing_cmd of nci_hmsgs.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-264879662	8.8	More Details
CVE-2023-29578	mp4v2 v2.0.0 was discovered to contain a heap buffer overflow via the mp4v2::impl::MP4StringProperty::~MP4StringProperty() function at src/mp4property.cpp.	8.8	More Details
CVE-2023-31061	Repetier Server through 1.4.10 does not have CSRF protection.	8.8	More Details
CVE-2023-0388	The Random Text WordPress plugin through 0.3.0 does not properly sanitize and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by any authenticated users, such as subscribers.	8.8	More Details
CVE-2023-27991	The post-authentication command injection vulnerability in the CLI command of Zyxel ATP series firmware versions 4.32 through 5.35, USG FLEX series firmware versions 4.50 through 5.35, USG FLEX 50(W) firmware versions 4.16 through 5.35, USG20(W)-VPN firmware versions 4.16 through 5.35, and VPN series firmware versions 4.30 through 5.35, which could allow an authenticated attacker to execute some OS commands remotely.	8.8	More Details
CVE-2023-20872	VMware Workstation and Fusion contain an out-of-bounds read/write vulnerability in SCSI CD/DVD device emulation.	8.8	More Details
CVE-2023-2133	Out of bounds memory access in Service Worker API in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-0184	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler which may lead to denial of service, escalation of privileges, information disclosure, and data tampering.	8.8	More Details
CVE-2023-2240	Improper Privilege Management in GitHub repository microweber/microweber prior to 1.3.4.	8.8	More Details
CVE-2023-27352	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Sonos One Speaker 70.3-35220. Authentication is not required to exploit this vulnerability. The specific flaw exists within the processing of the SMB directory query command. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-19845.	8.8	More Details
CVE-2023-24512	On affected platforms running Arista EOS, an authorized attacker with permissions to perform gNMI requests could craft a request allowing it to update arbitrary configurations in the switch. This situation occurs only when the Streaming Telemetry Agent (referred to as the TerminAttr agent) is enabled and gNMI access is configured on the agent. Note: This gNMI over the Streaming Telemetry Agent scenario is mostly commonly used when streaming to a 3rd party system and is not used by default when streaming to CloudVision	8.8	More Details
CVE-2023-27355	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Sonos One Speaker 70.3-35220. Authentication is not required to exploit this vulnerability. The specific flaw exists within the MPEG-TS parser. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-19773.	8.8	More Details
CVE-2023-26876	SQL injection vulnerability found in Piwigo v.13.5.0 and before allows a remote attacker to execute arbitrary code via the filter_user_id parameter to the admin.php?page=history&filter_image_id=&filter_user_id endpoint.	8.8	More Details
CVE-2023-2134	Out of bounds memory access in Service Worker API in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31223	Dradis before 4.8.0 allows persistent XSS by authenticated author users, related to avatars.	8.7	More Details
CVE-2021-23186	A sandboxing issue in Odoo Community 15.0 and earlier and Odoo Enterprise 15.0 and earlier allows authenticated administrators to access and modify database contents of other tenants, in a multi-tenant system.	8.7	More Details
CVE-2021-23166	A sandboxing issue in Odoo Community 15.0 and earlier and Odoo Enterprise 15.0 and earlier allows authenticated administrators to read and write local files on the server.	8.7	More Details
CVE-2023-30838	PrestaShop is an Open Source e-commerce web application. Prior to versions 8.0.4 and 1.7.8.9, the `ValidateCore::isCleanHTML()` method of Prestashop misses hijackable events which can lead to cross-site scripting (XSS) injection, allowed by the presence of pre-setup `@keyframes` methods. This XSS, which hijacks HTML attributes, can be triggered without any interaction by the visitor/administrator, which makes it as dangerous as a trivial XSS attack. Contrary to other attacks which target HTML attributes and are triggered without user interaction (such as onload / onerror which suffer from a very limited scope), this one can hijack every HTML element, which increases the danger due to a complete HTML elements scope. Versions 8.0.4 and 1.7.8.9 contain a fix for this issue.	8.5	More Details
CVE-2023-2141	An unsafe .NET object deserialization in DELMIA Apriso Release 2017 through Release 2022 could lead to post-authentication remote code execution.	8.5	More Details
CVE-2023-29521	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with view rights can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of `Macro.VFSTreeMacro`. This page is not installed by default.This vulnerability has been patched in XWiki 15.0-rc-1, 14.10.2, 14.4.8, 13.10.11. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.4	More Details
CVE-2023-26097	An issue was discovered in Telindus Apsal 3.14.2022.235 b. Unauthorized actions that could modify the application behaviour may not be blocked.	8.4	More Details
CVE-2023-20869	VMware Workstation (17.x) and VMware Fusion (13.x) contain a stack-based buffer-overflow vulnerability that exists in the functionality for sharing host Bluetooth devices with the virtual machine.	8.2	More Details
CVE-2023-0209	NVIDIA DGX-1 SBIOS contains a vulnerability in the Uncore PEI module, where authentication of the code executed by SSA is missing, which may lead to arbitrary code execution, denial of service, escalation of privileges assisted by a firmware implant, information disclosure assisted by a firmware implant, data tampering, and SecureBoot bypass.	8.2	More Details
CVE-2023-26098	An issue was discovered in the Open Document feature in Telindus Apsal 3.14.2022.235 b. An attacker may upload a crafted file to execute arbitrary code.	8.2	More Details
CVE-2023-30613	Kiwi TCMS, an open source test management system, allows users to upload attachments to test plans, test cases, etc. In versions of Kiwi TCMS prior to 12.2, there is no control over what kinds of files can be uploaded. Thus, a malicious actor may upload an `.exe` file or a file containing embedded JavaScript and trick others into clicking on these files, causing vulnerable browsers to execute malicious code on another computer. Kiwi TCMS v12.2 comes with functionality that allows administrators to configure additional upload validator functions which give them more control over what file types are accepted for upload. By default `.exe` are denied. Other files containing the `<script>` tag, regardless of their type are also denied b/c they are a path to XSS attacks. There are no known workarounds aside from upgrading.	8.1	More Details
CVE-2023-22916	The configuration parser of Zyxel ATP series firmware versions 5.10 through 5.35, USG FLEX series firmware versions 5.00 through 5.35, USG FLEX 50(W) firmware versions 5.10 through 5.35, USG20(W)-VPN firmware versions 5.10 through 5.35, and VPN series firmware versions 5.00 through 5.35, which fails to properly sanitize user input. A remote unauthenticated attacker could leverage the vulnerability to modify device configuration data, resulting in DoS conditions on an affected device if the attacker could trick an authorized administrator to switch the management mode to the cloud mode.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29019	@fastify/passport is a port of passport authentication library for the Fastify ecosystem. Applications using `@fastify/passport` in affected versions for user authentication, in combination with `@fastify/session` as the underlying session management mechanism, are vulnerable to session fixation attacks from network and same-site attackers. fastify applications rely on the `@fastify/passport` library for user authentication. The login and user validation are performed by the `authenticate` function. When executing this function, the `sessionId` is preserved between the pre-login and the authenticated session. Network and same-site attackers can hijack the victim's session by tossing a valid `sessionId` cookie in the victim's browser and waiting for the victim to log in on the website. As a solution, newer versions of `@fastify/passport` regenerate `sessionId` upon login, preventing the attacker-controlled pre-session cookie from being upgraded to an authenticated session. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.1	More Details
CVE-2023-22913	A post-authentication command injection vulnerability in the “account_operator.cgi” CGI program of Zyxel USG FLEX series firmware versions 4.50 through 5.35, and VPN series firmware versions 4.30 through 5.35, which could allow a remote authenticated attacker to modify device configuration data, resulting in denial-of-service (DoS) conditions on an affected device.	8.1	More Details
CVE-2022-36788	A heap-based buffer overflow vulnerability exists in the TriangleMesh clone functionality of Slic3r libslic3r 1.3.0 and Master Commit b1a5500. A specially-crafted STL file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger this vulnerability.	8.1	More Details
CVE-2021-45111	Improper access control in Odoo Community 15.0 and earlier and Odoo Enterprise 15.0 and earlier allows remote authenticated users to trigger the creation of demonstration data, including user accounts with known credentials.	8.1	More Details
CVE-2023-22645	An Improper Privilege Management vulnerability in SUSE kubewarden allows attackers to read arbitrary secrets if they get access to the ServiceAccount kubewarden-controller This issue affects: SUSE kubewarden kubewarden-controller versions prior to 1.6.0.	8.0	More Details
CVE-2021-0883	In PVRSRVBridgeCacheOpQueue of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270395013	7.8	More Details
CVE-2023-21094	In sanitize of LayerState.cpp, there is a possible way to take over the screen display and swap the display content 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-11 Android-12 Android-12L Android-13Android ID: A-248031255	7.8	More Details
CVE-2023-20967	In avdt_scb_hdl_pkt_no_frag of avdt_scb_act.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-225879503	7.8	More Details
CVE-2023-21081	In multiple functions of PackageInstallerService.java and related files, there is a possible way to bypass background activity launch restrictions 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-11 Android-12 Android-12L Android-13Android ID: A-230492955	7.8	More Details
CVE-2023-21083	In onNullBinding of CallScreeningServiceHelper.java, there is a possible way to record audio without showing a privacy indicator due to a permissions bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-252762941	7.8	More Details
CVE-2023-21086	In isToggleable of SecureNfcEnabler.java and SecureNfcPreferenceController.java, there is a possible way to enable NFC from a secondary account due to a permissions bypass. This could lead to local escalation of privilege from the Guest account with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-238298970	7.8	More Details
CVE-2023-21088	In deliverOnFlushComplete of LocationProviderManager.java, there is a possible way to bypass background activity launch restrictions 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-12 Android-12L Android-13Android ID: A-235823542	7.8	More Details
CVE-2023-21089	In startInstrumentation of ActivityManagerService.java, there is a possible way to keep the foreground service alive while the app is in the background. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-237766679	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47505	The SolarWinds Platform was susceptible to the Local Privilege Escalation Vulnerability. This vulnerability allows a local adversary with a valid system user account to escalate local privileges.	7.8	More Details
CVE-2023-2257	Authentication Bypass in Hub Business integration in Devolutions Workspace Desktop 2023.1.1.3 and earlier on Windows and macOS allows an attacker with access to the user interface to unlock a Hub Business space without being prompted to enter the password via an unimplemented "Force Login" security feature. This vulnerability occurs only if "Force Login" feature is enabled on the Hub Business instance and that an attacker has access to a locked Workspace desktop application configured with a Hub Business space.	7.8	More Details
CVE-2023-21092	In retrieveServiceLocked of ActiveServices.java, there is a possible way to dynamically register a BroadcastReceiver using permissions of System App 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-11 Android-12 Android-12L Android-13Android ID: A-242040055	7.8	More Details
CVE-2023-21093	In extractRelativePath of FileUtils.java, there is a possible way to access files in a directory belonging to other applications due to a path traversal error. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-228450832	7.8	More Details
CVE-2023-21097	In toUriInner of Intent.java, there is a possible way to launch an arbitrary activity due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261858325	7.8	More Details
CVE-2023-20871	VMware Fusion contains a local privilege escalation vulnerability. A malicious actor with read/write access to the host operating system can elevate privileges to gain root access to the host operating system.	7.8	More Details
CVE-2023-21098	In multiple functions of AccountManagerService.java, there is a possible loading of arbitrary code into the System Settings app due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-260567867	7.8	More Details
CVE-2023-21099	In multiple methods of PackageInstallerSession.java, there is a possible way to start foreground services from 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-11 Android-12 Android-12L Android-13Android ID: A-243377226	7.8	More Details
CVE-2023-21100	In inflate of inflate.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-242544249	7.8	More Details
CVE-2023-28122	A local privilege escalation (LPE) vulnerability in UI Desktop for Windows (Version 0.59.1.71 and earlier) allows a malicious actor with local access to a Windows device running said application to submit arbitrary commands as SYSTEM.This vulnerability is fixed in Version 0.62.3 and later.	7.8	More Details
CVE-2023-30533	SheetJS Community Edition before 0.19.3 allows Prototype Pollution via a crafted file. In other words. 0.19.2 and earlier are affected, whereas 0.19.3 and later are unaffected.	7.8	More Details
CVE-2023-28088	An HPE OneView appliance dump may expose SAN switch administrative credentials	7.8	More Details
CVE-2021-33973	Buffer Overflow vulnerability in Qihoo 360 Safe guard v12.1.0.1004, v12.1.0.1005, v13.1.0.1001 allows attacker to escalate priveleges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33971	Qihoo 360 (https://www.360.cn/) Qihoo 360 Safeguard (https://www.360.cn/) Qihoo 360 Total Security (http://www.360totalsecurity.com/) is affected by: Buffer Overflow. The impact is: execute arbitrary code (local). The component is: This is a set of vulnerabilities affecting popular software, "360 Safeguard(12.1.0.1004,12.1.0.1005,13.1.0.1001)" , "360 Total Security(10.8.0.1060,10.8.0.1213)", "360 Safe Browser & 360 Chrome(13.0.2170.0)". The attack vector is: On the browser vulnerability, just open a link to complete the vulnerability exploitation remotely; on the client software, you need to locally execute the vulnerability exploitation program, which of course can be achieved with the full chain of browser vulnerability. ¶¶ This is a set of the most serious vulnerabilities that exist on Qihoo 360's PC client a variety of popular software, remote vulnerabilities can be completed by opening a link to arbitrary code execution on both security browsers, with the use of local vulnerabilities, not only help the vulnerability code constitutes an escalation of privileges, er can make the spyware persistent without being scanned permanently resides on the target PC computer (because local vulnerability against Qihoo 360 company's antivirus kernel flaws); this group of remote and local vulnerability of the perfect match, to achieve an information security fallacy, in Qihoo 360's antivirus vulnerability, not only can not be scanned out of the virus, but will help the virus persistently control the target computer, while Qihoo 360 claims to be a safe browser, which exists in the kernel vulnerability but helped the composition of the remote vulnerability. (Security expert "Memory Corruptor" have reported this set of vulnerabilities to the corresponding vendor, all vulnerabilities have been fixed and the vendor rewarded thousands of dollars to the security experts)	7.8	More Details
CVE-2023-25505	NVIDIA DGX-1 BMC contains a vulnerability in the IPMI handler of the AMI MegaRAC BMC , where an attacker with the appropriate level of authorization can cause a buffer overflow, which may lead to denial of service, information disclosure, or arbitrary code execution.	7.8	More Details
CVE-2023-20950	In AlarmManagerActivity of AlarmManagerActivity.java, there is a possible way to bypass background activity launch restrictions via a pendingIntent. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-195756028	7.8	More Details
CVE-2022-31244	Nokia OneNDS 17r2 has Insecure Permissions vulnerability that allows for privilege escalation.	7.8	More Details
CVE-2021-0876	In PVRSRVBridgePhysmemNewRamBackedLockedPMR of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270400229	7.8	More Details
CVE-2021-0881	In PVRSRVBridgeRGXKickCDM of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270396350	7.8	More Details
CVE-2023-1900	A vulnerability within the Avira network protection feature allowed an attacker with local execution rights to cause an overflow. This could corrupt the data on the heap and lead to a denial-of-service situation. Issue was fixed with Endpointprotection.exe version 1.0.2303.633	7.8	More Details
CVE-2021-0872	In PVRSRVBridgeRGXKickVRDM of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270401229	7.8	More Details
CVE-2021-0873	In PVRSRVBridgeRGXKickRS of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270392711	7.8	More Details
CVE-2021-0874	In PVRSRVBridgeDevicememHistorySparseChange of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270399633	7.8	More Details
CVE-2021-0875	In PVRSRVBridgeChangeSparseMem of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270400061	7.8	More Details
CVE-2021-0878	In PVRSRVBridgeServerSyncGetStatus of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270399153	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0879	In PVRSRVBridgeRGXTDMSubmitTransfer of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270397970	7.8	More Details
CVE-2021-0880	In PVRSRVBridgeRGXKickTA3D of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270396792	7.8	More Details
CVE-2021-0882	In PVRSRVBridgeRGXKickSync of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270395803	7.8	More Details
CVE-2023-25348	ChurchCRM 4.5.3 was discovered to contain a CSV injection vulnerability via the Last Name and First Name input fields when creating a new person. These vulnerabilities allow attackers to execute arbitrary code via a crafted excel file.	7.8	More Details
CVE-2022-42335	x86 shadow paging arbitrary pointer dereference In environments where host assisted address translation is necessary but Hardware Assisted Paging (HAP) is unavailable, Xen will run guests in so called shadow mode. Due to too lax a check in one of the hypervisor routines used for shadow page handling it is possible for a guest with a PCI device passed through to cause the hypervisor to access an arbitrary pointer partially under guest control.	7.8	More Details
CVE-2021-0884	In PVRSRVBridgePhysmemImportSparseDmaBuf of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270393454	7.8	More Details
CVE-2023-2176	A vulnerability was found in compare_netdev_and_ip in drivers/infiniband/core/cma.c in RDMA in the Linux Kernel. The improper cleanup results in out-of-boundary read, where a local user can utilize this problem to crash the system or escalation of privilege.	7.8	More Details
CVE-2021-0885	In PVRSRVBridgeSyncPrimOpTake of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270401914	7.8	More Details
CVE-2023-2007	The specific flaw exists within the DPT I2O Controller driver. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the kernel.	7.8	More Details
CVE-2023-23579	Datakit CrossCadWare_x64.dll contains an out-of-bounds write past the end of an allocated buffer while parsing a specially crafted SLDPRT file. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-30545	PrestaShop is an Open Source e-commerce web application. Prior to versions 8.0.4 and 1.7.8.9, it is possible for a user with access to the SQL Manager (Advanced Options -> Database) to arbitrarily read any file on the operating system when using SQL function `LOAD_FILE` in a `SELECT` request. This gives the user access to critical information. A patch is available in PrestaShop 8.0.4 and PS 1.7.8.9	7.7	More Details
CVE-2022-40722	A misconfiguration of RSA padding implemented in the PingID Adapter for PingFederate to support Offline MFA with PingID mobile authenticators is vulnerable to pre-computed dictionary attacks, leading to a bypass of offline MFA.	7.7	More Details
CVE-2023-29515	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user who can create a space can become admin of that space through App Within Minutes. The admin right implies the script right and thus allows JavaScript injection. The vulnerability can be exploited by creating an app in App Within Minutes. If the button should be disabled because the user doesn't have global edit right, the app can also be created by directly opening `/xwiki/bin/view/AppWithinMinutes/CreateApplication?wizard=true` on the XWiki installation. This has been patched in XWiki 13.10.11, 14.4.8, 14.10.1 and 15.0 RC1 by not granting the space admin right if the user doesn't have script right on the space where the app is created. Error message are displayed to warn the user that the app will be broken in this case. Users who became space admin through this vulnerability won't loose the space admin right due to the fix, so it is advised to check if all users who created AWM apps should keep their space admin rights. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30620	mindsdb is a Machine Learning platform to help developers build AI solutions. In affected versions an unsafe extraction is being performed using `tarfile.extractall()` from a remotely retrieved tarball. Which may lead to the writing of the extracted files to an unintended location. Sometimes, the vulnerability is called a TarSlip or a ZipSlip variant. An attacker may leverage this vulnerability to overwrite any local file which the server process has access to. There is no risk of file exposure with this vulnerability. This issue has been addressed in release `23.2.1.0 `. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.5	More Details
CVE-2023-27351	This vulnerability allows remote attackers to bypass authentication on affected installations of PaperCut NG 22.0.5 (Build 63914). Authentication is not required to exploit this vulnerability. The specific flaw exists within the SecurityRequestFilter class. The issue results from improper implementation of the authentication algorithm. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-19226.	7.5	More Details
CVE-2023-26101	In Progress Flowmon Packet Investigator before 12.1.0, a Flowmon user with access to Flowmon Packet Investigator could leverage a path-traversal vulnerability to retrieve files on the Flowmon appliance's local filesystem.	7.5	More Details
CVE-2021-33589	Ribose RNP before 0.15.1 does not implement a required step in a cryptographic algorithm, resulting in weaker encryption than on the tin of the algorithm.	7.5	More Details
CVE-2023-26557	io.finnet tss-lib before 2.0.0 can leak the lambda value of a private key via a timing side-channel attack because it relies on Go big.Int, which is not constant time for Cmp, modular exponentiation, or modular inverse. An example leak is in crypto/paillier/paillier.go. (bnb-chain/tss-lib and thorchain/tss are also affected.)	7.5	More Details
CVE-2023-30798	There MultipartParser usage in Encode's Starlette python framework before versions 0.25.0 allows an unauthenticated and remote attacker to specify any number of form fields or files which can cause excessive memory usage resulting in denial of service of the HTTP service.	7.5	More Details
CVE-2023-25652	Git is a revision control system. Prior to versions 2.30.9, 2.31.8, 2.32.7, 2.33.8, 2.34.8, 2.35.8, 2.36.6, 2.37.7, 2.38.5, 2.39.3, and 2.40.1, by feeding specially crafted input to `git apply --reject`, a path outside the working tree can be overwritten with partially controlled contents (corresponding to the rejected hunk(s) from the given patch). A fix is available in versions 2.30.9, 2.31.8, 2.32.7, 2.33.8, 2.34.8, 2.35.8, 2.36.6, 2.37.7, 2.38.5, 2.39.3, and 2.40.1. As a workaround, avoid using `git apply` with `--reject` when applying patches from an untrusted source. Use `git apply --stat` to inspect a patch before applying; avoid applying one that create a conflict where a link corresponding to the `*.rej` file exists.	7.5	More Details
CVE-2023-2140	A Server-Side Request Forgery vulnerability in DELMIA Apriso Release 2017 through Release 2022 could allow an unauthenticated attacker to issue requests to arbitrary hosts on behalf of the server running the DELMIA Apriso application.	7.5	More Details
CVE-2023-29011	Git for Windows, the Windows port of Git, ships with an executable called `connect.exe`, which implements a SOCKS5 proxy that can be used to connect e.g. to SSH servers via proxies when certain ports are blocked for outgoing connections. The location of `connect.exe`'s config file is hard-coded as `/etc/connectrc` which will typically be interpreted as `C:\etc\connectrc`. Since `C:\etc` can be created by any authenticated user, this makes `connect.exe` susceptible to malicious files being placed there by other users on the same multi-user machine. The problem has been patched in Git for Windows v2.40.1. As a workaround, create the folder `etc` on all drives where Git commands are run, and remove read/write access from those folders. Alternatively, watch out for malicious `<drive>:\etc\connectrc` files on multi-user machines.	7.5	More Details
CVE-2023-0202	NVIDIA DGX A100 SBIOS contains a vulnerability where an attacker may modify arbitrary memory of SMRAM by exploiting the GenericSio and LegacySmmSredir SMM APIs. A successful exploit of this vulnerability may lead to denial of service, escalation of privileges, and information disclosure.	7.5	More Details
CVE-2023-0200	NVIDIA DGX-2 contains a vulnerability in OFBD where a user with high privileges and a pre-conditioned heap can cause an access beyond a buffers end, which may lead to code execution, escalation of privileges, denial of service, and information disclosure.	7.5	More Details
CVE-2023-29780	Third Reality Smart Blind 1.00.54 contains a denial-of-service vulnerability, which allows a remote attacker to send malicious Zigbee messages to a vulnerable device and cause crashes.	7.5	More Details
CVE-2023-0206	NVIDIA DGX A100 SBIOS contains a vulnerability where an attacker may modify arbitrary memory of SMRAM by exploiting the NVME SMM API. A successful exploit of this vulnerability may lead to denial of service, escalation of privileges, and information disclosure.	7.5	More Details
CVE-2023-0207	NVIDIA DGX-2 SBIOS contains a vulnerability where an attacker may modify the ServerSetup NVRAM variable at runtime by executing privileged code. A successful exploit of this vulnerability may lead to denial of service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29530	Laminas Diactoros provides PSR HTTP Message implementations. In versions 2.18.0 and prior, 2.19.0, 2.20.0, 2.21.0, 2.22.0, 2.23.0, 2.24.0, and 2.25.0, users who create HTTP requests or responses using laminas/laminas-diactoros, when providing a newline at the start or end of a header key or value, can cause an invalid message. This can lead to denial of service vectors or application errors. The problem has been patched in following versions 2.18.1, 2.19.1, 2.20.1, 2.21.1, 2.22.1, 2.23.1, 2.24.1, and 2.25.1. As a workaround, validate HTTP header keys and/or values, and if using user-supplied values, filter them to strip off leading or trailing newline characters before calling `withHeader()`.	7.5	More Details
CVE-2023-30629	Vyper is a Pythonic Smart Contract Language for the ethereum virtual machine. In versions 0.3.1 through 0.3.7, the Vyper compiler generates the wrong bytecode. Any contract that uses the `raw_call` with `revert_on_failure=False` and `max_outsize=0` receives the wrong response from `raw_call`. Depending on the memory garbage, the result can be either `True` or `False`. A patch is available and, as of time of publication, anticipated to be part of Vyper 0.3.8. As a workaround, one may always put `max_outsize>0`.	7.5	More Details
CVE-2023-22917	A buffer overflow vulnerability in the “sdwan_iface_ipc” binary of Zyxel ATP series firmware versions 5.10 through 5.32, USG FLEX series firmware versions 5.00 through 5.32, USG FLEX 50(W) firmware versions 5.10 through 5.32, USG20(W)-VPN firmware versions 5.10 through 5.32, and VPN series firmware versions 5.00 through 5.35, which could allow a remote unauthenticated attacker to cause a core dump with a request error message on a vulnerable device by uploading a crafted configuration file.	7.5	More Details
CVE-2023-22915	A buffer overflow vulnerability in the “fbwifi_forward.cgi” CGI program of Zyxel USG FLEX series firmware versions 4.50 through 5.35, USG FLEX 50(W) firmware versions 4.30 through 5.35, USG20(W)-VPN firmware versions 4.30 through 5.35, and VPN series firmware versions 4.30 through 5.35, which could allow a remote unauthenticated attacker to cause DoS conditions by sending a crafted HTTP request if the Facebook WiFi function were enabled on an affected device.	7.5	More Details
CVE-2023-29779	Sengled Dimmer Switch V0.0.9 contains a denial of service (DOS) vulnerability, which allows a remote attacker to send malicious Zigbee messages to a vulnerable device and cause crashes. After receiving the malicious command, the device will keep reporting its status and finally drain its battery after receiving the 'Set_short_poll_interval' command.	7.5	More Details
CVE-2023-24822	RIOT-OS, an operating system that supports Internet of Things devices, contains a network stack with the ability to process 6LoWPAN frames. Prior to version 2022.10, an attacker can send a crafted frame to the device resulting in a NULL pointer dereference while encoding a 6LoWPAN IPHC header. The NULL pointer dereference causes a hard fault exception, leading to denial of service. Version 2022.10 fixes this issue. As a workaround, apply the patches manually.	7.5	More Details
CVE-2023-24821	RIOT-OS, an operating system that supports Internet of Things devices, contains a network stack with the ability to process 6LoWPAN frames. Prior to version 2022.10, an attacker can send a crafted frame to the device resulting in a large out of bounds write beyond the packet buffer. The write will create a hard fault exception after reaching the last page of RAM. The hard fault is not handled and the system will be stuck until reset, thus the impact is denial of service. Version 2022.10 fixes this issue. As a workaround, disable support for fragmented IP datagrams or apply the patches manually.	7.5	More Details
CVE-2023-2251	Uncaught Exception in GitHub repository eemeli/yaml prior to 2.0.0-5.	7.5	More Details
CVE-2023-29480	Ribose RNP before 0.16.3 sometimes lets secret keys remain unlocked after use.	7.5	More Details
CVE-2023-24820	RIOT-OS, an operating system that supports Internet of Things devices, contains a network stack with the ability to process 6LoWPAN frames. An attacker can send a crafted frame to the device resulting in a large out of bounds write beyond the packet buffer. The write will create a hard fault exception after reaching the last page of RAM. The hard fault is not handled and the system will be stuck until reset. Thus the impact is denial of service. Version 2022.10 fixes this issue. As a workaround, apply the patch manually.	7.5	More Details
CVE-2023-29552	The Service Location Protocol (SLP, RFC 2608) allows an unauthenticated, remote attacker to register arbitrary services. This could allow the attacker to use spoofed UDP traffic to conduct a denial-of-service attack with a significant amplification factor.	7.5	More Details
CVE-2023-24818	RIOT-OS, an operating system that supports Internet of Things devices, contains a network stack with the ability to process 6LoWPAN frames. Prior to version 2022.10, an attacker can send a crafted frame to the device resulting in a NULL pointer dereference. During forwarding of a fragment an uninitialized entry in the reassembly buffer is used. The NULL pointer dereference triggers a hard fault exception resulting in denial of service. Version 2022.10 fixes this issue. As a workaround, disable support for fragmented IP datagrams or apply the patches manually.	7.5	More Details
CVE-2023-23837	No exception handling vulnerability which revealed sensitive or excessive information to users.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31059	Repetier Server through 1.4.10 allows ..%5c directory traversal for reading files that contain credentials, as demonstrated by connectionLost.php.	7.5	More Details
CVE-2023-31043	EnterpriseDB EDB Postgres Advanced Server (EPAS) before 14.6.0 logs unredacted passwords in situations where optional parameters are used with CREATE/ALTER USER/GROUP/ROLE, and redacting was configured with edb_filter_log.redact_password_commands. The fixed versions are 10.23.33, 11.18.29, 12.13.17, 13.9.13, and 14.6.0.	7.5	More Details
CVE-2021-23178	Improper access control in Odoo Community 15.0 and earlier and Odoo Enterprise 15.0 and earlier allows attackers to validate online payments with a tokenized payment method that belongs to another user, causing the victim's payment method to be charged instead.	7.5	More Details
CVE-2021-23203	Improper access control in reporting engine of Odoo Community 14.0 through 15.0, and Odoo Enterprise 14.0 through 15.0, allows remote attackers to download PDF reports for arbitrary documents, via crafted requests.	7.5	More Details
CVE-2022-48476	In JetBrains Ktor before 2.3.0 path traversal in the `resolveResource` method was possible	7.5	More Details
CVE-2023-25506	NVIDIA DGX-1 contains a vulnerability in Ofbd in AMI SBIOS, where a preconditioned heap can allow a user with elevated privileges to cause an access beyond the end of a buffer, which may lead to code execution, escalation of privileges, denial of service and information disclosure. The scope of the impact of this vulnerability can extend to other components.	7.5	More Details
CVE-2023-30463	Altran picoTCP through 1.7.0 allows memory corruption (and subsequent denial of service) because of an integer overflow in pico_ipv6_alloc when processing large ICMPv6 packets. This affects installations with Ethernet support in which a packet size greater than 65495 may occur.	7.5	More Details
CVE-2022-29608	An issue was discovered in ONOS 2.5.1. An intent with a port that is an intermediate point of its path installs an invalid flow rule, causing a network loop.	7.5	More Details
CVE-2022-24035	An issue was discovered in ONOS 2.5.1. The purge-requested intent remains on the list, but it does not respond to changes in topology (e.g., link failure). In combination with other applications, it could lead to a failure of network management.	7.5	More Details
CVE-2023-22893	Strapi through 4.5.5 does not verify the access or ID tokens issued during the OAuth flow when the AWS Cognito login provider is used for authentication. A remote attacker could forge an ID token that is signed using the 'None' type algorithm to bypass authentication and impersonate any user that use AWS Cognito for authentication.	7.5	More Details
CVE-2021-43819	Stargate-Bukkit is a mod for the minecraft video game which adds a portal focused environment. In affected versions Minecarts with chests will drop their items when teleporting through a portal; when they reappear, they will still have their items impacting the integrity of the game world. The teleport code has since been rewritten and is available in release `0.11.5.1`. Users are advised to upgrade. There are no known workarounds for this issue.	7.5	More Details
CVE-2022-29605	An issue was discovered in ONOS 2.5.1. IntentManager attempts to install the IPv6 flow rules of an intent into an OpenFlow 1.0 switch that does not support IPv6. Improper handling of the difference in capabilities of the intent and switch is misleading to a network operator.	7.5	More Details
CVE-2021-38363	An issue was discovered in ONOS 2.5.1. In IntentManager, the install-requested intent (which causes an exception) remains in pendingMap (in memory) forever. Deletion is possible neither by a user nor by the intermittent Intent Cleanup process.	7.5	More Details
CVE-2022-29607	An issue was discovered in ONOS 2.5.1. Modification of an existing intent to have the same source and destination shows the INSTALLED state without any flow rule. Improper handling of such an intent is misleading to a network operator.	7.5	More Details
CVE-2023-25619	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when communicating over the Modbus TCP protocol.	7.5	More Details
CVE-2023-2135	Use after free in DevTools in Google Chrome prior to 112.0.5615.137 allowed a remote attacker who convinced a user to enable specific preconditions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2023-30797	Netflix Lemur before version 1.3.2 used insufficiently random values when generating default credentials. The insufficiently random values may allow an attacker to guess the credentials and gain access to resources managed by Lemur.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0383	User-controlled operations could have allowed Denial of Service in M-Files Server before 23.4.12528.1 due to uncontrolled memory consumption.	7.5	More Details
CVE-2023-29517	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. The office document viewer macro was allowing anyone to see any file content from the hosting server, provided that the office server was connected and depending on the permissions of the user running the servlet engine (e.g. tomcat) running XWiki. The same vulnerability also allowed to perform internal requests to resources from the hosting server. The problem has been patched in XWiki 13.10.11, 14.10.1, 14.4.8, 15.0-rc-1. Users are advised to upgrade. It might be possible to workaround this vulnerability by running XWiki in a sandbox with a user with very low privileges on the machine.	7.5	More Details
CVE-2022-40725	PingID Desktop prior to the latest released version 1.7.4 contains a vulnerability that can be exploited to bypass the maximum PIN attempts permitted before the time-based lockout is activated.	7.3	More Details
CVE-2023-28047	Dell Display Manager, versions 2.1.0 and prior, contains an arbitrary file or folder creation vulnerability during installation. A local low privilege attacker could potentially exploit this vulnerability, leading to the execution of arbitrary code on the operating system with high privileges.	7.3	More Details
CVE-2023-2259	Improper Neutralization of Special Elements Used in a Template Engine in GitHub repository alfio-event/alf.io prior to 2.0-M4-2304.	7.2	More Details
CVE-2023-22621	Strapi through 4.5.5 allows authenticated Server-Side Template Injection (SSTI) that can be exploited to execute arbitrary code on the server. A remote attacker with access to the Strapi admin panel can inject a crafted payload that executes code on the server into an email template that bypasses the validation checks that should prevent code execution.	7.2	More Details
CVE-2022-36963	The SolarWinds Platform was susceptible to the Command Injection Vulnerability. This vulnerability allows a remote adversary with a valid SolarWinds Platform admin account to execute arbitrary commands.	7.2	More Details
CVE-2023-25507	NVIDIA DGX-1 BMC contains a vulnerability in the SPX REST API, where an attacker with the appropriate level of authorization can inject arbitrary shell commands, which may lead to code execution, denial of service, information disclosure, and data tampering.	7.2	More Details
CVE-2022-45291	PWS Personal Weather Station Dashboard (PWS_Dashboard) LTS December 2020 (2012_lts) allows remote code execution by injecting PHP code into settings.php. Attacks can use the PWS_printfile.php, PWS_frame_text.php, PWS_listfile.php, PWS_winter.php, and PWS_easyweathersetup.php endpoints. A contributing factor is a hardcoded login password of support, which is not documented. (This is not the same as the documented setup password, which is 12345.) The issue was fixed in late 2022.	7.2	More Details
CVE-2023-22914	A path traversal vulnerability in the “account_print.cgi” CGI program of Zyxel USG FLEX series firmware versions 4.50 through 5.35, and VPN series firmware versions 4.30 through 5.35, which could allow a remote authenticated attacker with administrator privileges to execute unauthorized OS commands in the “tmp” directory by uploading a crafted file if the hotspot function were enabled.	7.2	More Details
CVE-2023-1731	In Meinbergs LTOS versions prior to V7.06.013, the configuration file upload function would not correctly validate the input, which would allow an remote authenticated attacker with high privileges to execute arbitrary commands.	7.2	More Details
CVE-2023-29012	Git for Windows is the Windows port of Git. Prior to version 2.40.1, any user of Git CMD who starts the command in an untrusted directory is impacted by an Uncontrolles Search Path Element vulnerability. Maliciously-placed `doskey.exe` would be executed silently upon running Git CMD. The problem has been patched in Git for Windows v2.40.1. As a workaround, avoid using Git CMD or, if using Git CMD, avoid starting it in an untrusted directory.	7.2	More Details
CVE-2023-20865	VMware Aria Operations for Logs contains a command injection vulnerability. A malicious actor with administrative privileges in VMware Aria Operations for Logs can execute arbitrary commands as root.	7.2	More Details
CVE-2023-28089	An HPE OneView appliance dump may expose FTP credentials for c7000 Interconnect Modules	7.1	More Details
CVE-2022-45084	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Softaculous Loginizer plugin <= 1.7.5 versions.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30549	Apptainer is an open source container platform for Linux. There is an ext4 use-after-free flaw that is exploitable through versions of Apptainer < 1.1.0 and installations that include apptainer-suid < 1.1.8 on older operating systems where that CVE has not been patched. That includes Red Hat Enterprise Linux 7, Debian 10 buster (unless the linux-5.10 package is installed), Ubuntu 18.04 bionic and Ubuntu 20.04 focal. Use-after-free flaws in the kernel can be used to attack the kernel for denial of service and potentially for privilege escalation. Apptainer 1.1.8 includes a patch that by default disables mounting of extfs filesystem types in setuid-root mode, while continuing to allow mounting of extfs filesystems in non-setuid "rootless" mode using fuse2fs. Some workarounds are possible. Either do not install apptainer-suid (for versions 1.1.0 through 1.1.7) or set `allow setuid = no` in apptainer.conf. This requires having unprivileged user namespaces enabled and except for apptainer 1.1.x versions will disallow mounting of sif files, extfs files, and squashfs files in addition to other, less significant impacts. (Encrypted sif files are also not supported unprivileged in apptainer 1.1.x.). Alternatively, use the `limit containers` options in apptainer.conf/singularity.conf to limit sif files to trusted users, groups, and/or paths, and set `allow container extfs = no` to disallow mounting of extfs overlay files. The latter option by itself does not disallow mounting of extfs overlay partitions inside SIF files, so that's why the former options are also needed.	7.1	More Details
CVE-2022-45837	Reflected Cross-Site Scripting (XSS) vulnerability in Denis 微信机器人高级版 plugin <= 6.0.1 versions.	7.1	More Details
CVE-2023-22718	Reflected Cross-Site Scripting (XSS) vulnerability in Jason Lau User Meta Manager plugin <= 3.4.9 versions.	7.1	More Details
CVE-2023-24404	Reflected Cross-Site Scripting (XSS) vulnerability in VryaSage Marketing Performance plugin <= 2.0.0 versions.	7.1	More Details
CVE-2023-30614	Pay is a payments engine for Ruby on Rails 6.0 and higher. In versions prior to 6.3.2 a payments info page of Pay is susceptible to reflected Cross-site scripting. An attacker could create a working URL that renders a javascript link to a user on a Rails application that integrates Pay. This URL could be distributed via email to specifically target certain individuals. If the targeted application contains a functionality to submit user-generated content (such as comments) the attacker could even distribute the URL using that functionality. This has been patched in version 6.3.2 and above. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.1	More Details
CVE-2023-2006	A race condition was found in the Linux kernel's RxRPC network protocol, within the processing of RxRPC bundles. This issue results from the lack of proper locking when performing operations on an object. This may allow an attacker to escalate privileges and execute arbitrary code in the context of the kernel.	7.0	More Details
CVE-2023-29007	Git is a revision control system. Prior to versions 2.30.9, 2.31.8, 2.32.7, 2.33.8, 2.34.8, 2.35.8, 2.36.6, 2.37.7, 2.38.5, 2.39.3, and 2.40.1, a specially crafted `.gitmodules` file with submodule URLs that are longer than 1024 characters can used to exploit a bug in `config.c::git_config_copy_or_rename_section_in_file()`. This bug can be used to inject arbitrary configuration into a user's `$GIT_DIR/config` when attempting to remove the configuration section associated with that submodule. When the attacker injects configuration values which specify executables to run (such as `core.pager`, `core.editor`, `core.sshCommand`, etc.) this can lead to a remote code execution. A fix A fix is available in versions 2.30.9, 2.31.8, 2.32.7, 2.33.8, 2.34.8, 2.35.8, 2.36.6, 2.37.7, 2.38.5, 2.39.3, and 2.40.1. As a workaround, avoid running `git submodule deinit` on untrusted repositories or without prior inspection of any submodule sections in `$GIT_DIR/config`.	7.0	More Details
CVE-2023-2228	Cross-Site Request Forgery (CSRF) in GitHub repository modoboa/modoboa prior to 2.1.0.	6.8	More Details
CVE-2023-26060	An issue was discovered in Nokia NetAct before 22 FP2211. On the Working Set Manager page, users can create a Working Set with a name that has a client-side template injection payload. Input validation is missing during creation of the working set. For an external attacker, it is very difficult to exploit this, because a few dynamically created parameters such as Jsession-id, a CSRF token, and an Nxsrf token would be needed. The attack can realistically only be performed by an internal user.	6.8	More Details
CVE-2022-47930	An issue was discovered in IO FinNet tss-lib before 2.0.0. The parameter ssid for defining a session id is not used through the MPC implementation, which makes replaying and spoofing of messages easier. In particular, the Schnorr proof of knowledge implemented in sch.go does not utilize a session id, context, or random nonce in the generation of the challenge. This could allow a malicious user or an eavesdropper to replay a valid proof sent in the past.	6.8	More Details
CVE-2021-44476	A sandboxing issue in Odoo Community 15.0 and earlier and Odoo Enterprise 15.0 and earlier allows authenticated administrators to read local files on the server, including sensitive configuration files.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26059	An issue was discovered in Nokia NetAct before 22 SP1037. On the Site Configuration Tool tab, attackers can upload a ZIP file which, when processed, exploits Stored XSS. The upload option of the Site Configuration tool does not validate the file contents. The application is in a demilitarised zone behind a perimeter firewall and without exposure to the internet. The attack can only be performed by an internal user.	6.8	More Details
CVE-2023-26061	An issue was discovered in Nokia NetAct before 22 FP2211. On the Scheduled Search tab under the Alarm Reports Dashboard page, users can create a script to inject XSS. Input validation was missing during creation of a scheduled task. For an external attacker, it is very difficult to exploit this, because a few dynamically created parameters such as Jsession-id, a CSRF token, and an Nxsrf token would be needed. The attack can realistically only be performed by an internal user.	6.8	More Details
CVE-2023-21084	In buildPropFile of filesystem.go, there is a possible insecure hash due to an improperly used crypto. 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-262892300	6.7	More Details
CVE-2023-25508	NVIDIA DGX-1 BMC contains a vulnerability in the IPMI handler, where an attacker with the appropriate level of authorization can upload and download arbitrary files under certain circumstances, which may lead to denial of service, escalation of privileges, information disclosure, and data tampering.	6.7	More Details
CVE-2023-0201	NVIDIA DGX-2 SBIOS contains a vulnerability in Bds, where a user with high privileges can cause a write beyond the bounds of an indexable resource, which may lead to code execution, denial of service, compromised integrity, and information disclosure.	6.7	More Details
CVE-2023-2194	An out-of-bounds write vulnerability was found in the Linux kernel's SLIMpro I2C device driver. The userspace "data->block[0]" variable was not capped to a number between 0-255 and was used as the size of a memcpy, possibly writing beyond the end of dma_buffer. This flaw could allow a local privileged user to crash the system or potentially achieve code execution.	6.7	More Details
CVE-2023-30622	Clusternet is a general-purpose system for controlling Kubernetes clusters across different environments. An issue in clusternet prior to version 0.15.2 can be leveraged to lead to a cluster-level privilege escalation. The clusternet has a deployment called `cluster-hub` inside the `clusternet-system` Kubernetes namespace, which runs on worker nodes randomly. The deployment has a service account called `clusternet-hub`, which has a cluster role called `clusternet:hub` via cluster role binding. The `clusternet:hub` cluster role has `"*" verbs of "*.*"` resources. Thus, if a malicious user can access the worker node which runs the clusternet, they can leverage the service account to do malicious actions to critical system resources. For example, the malicious user can leverage the service account to get ALL secrets in the entire cluster, resulting in cluster-level privilege escalation. Version 0.15.2 contains a fix for this issue.	6.7	More Details
CVE-2023-2250	A flaw was found in the Open Cluster Management (OCM) when a user have access to the worker nodes which has the cluster-manager-registration-controller or cluster-manager deployments. A malicious user can take advantage of this and bind the cluster-admin to any service account or using the service account to list all secrets for all kubernetes namespaces, leading into a cluster-level privilege escalation.	6.7	More Details
CVE-2023-20941	In acc_ctrlrequest_composite of f_accessory.c, there is a possible out of bounds write due to a missing bounds check. This could lead to physical escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-264029575References: Upstream kernel	6.6	More Details
CVE-2021-44460	Improper access control in Odoo Community 13.0 and earlier and Odoo Enterprise 13.0 and earlier allows users with deactivated accounts to access the system with the deactivated account and any permission it still holds, via crafted RPC requests.	6.5	More Details
CVE-2023-29020	@fastify/passport is a port of passport authentication library for the Fastify ecosystem. The CSRF (Cross-Site Request Forger) protection enforced by the `@fastify/csrf-protection` library, when combined with `@fastify/passport` in affected versions, can be bypassed by network and same-site attackers. `fastify/csrf-protection` implements the synchronizer token pattern (using plugins `@fastify/session` and `@fastify/secure-session`) by storing a random value used for CSRF token generation in the `_csrf` attribute of a user's session. The `@fastify/passport` library does not clear the session object upon authentication, preserving the `_csrf` attribute between pre-login and authenticated sessions. Consequently, CSRF tokens generated before authentication are still valid. Network and same-site attackers can thus obtain a CSRF token for their pre-session, fixate that pre-session in the victim's browser via cookie tossing, and then perform a CSRF attack after the victim authenticates. As a solution, newer versions of `@fastify/passport` include the configuration options: `clearSessionOnLogin (default: true)` and `clearSessionIgnoreFields (default: ['passport', 'session'])` to clear all the session attributes by default, preserving those explicitly defined in `clearSessionIgnoreFields`.	6.5	More Details
CVE-2023-0204	NVIDIA ConnectX-5, ConnectX-6, and ConnectX6-DX contain a vulnerability in the NIC firmware, where an unprivileged user can cause improper handling of exceptional conditions, which may lead to denial of service.	6.5	More Details
CVE-2023-1129	The WP FEvents Book WordPress plugin through 0.46 does not ensures that bookings to be updated belong to the user making the request, allowing any authenticated user to book, add notes, or cancel booking on behalf of other users.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23176	Improper access control in reporting engine of l10n_fr_fec module in Odoo Community 15.0 and earlier and Odoo Enterprise 15.0 and earlier allows remote authenticated users to extract accounting information via crafted RPC packets.	6.5	More Details
CVE-2023-1586	Avast and AVG Antivirus for Windows were susceptible to a Time-of-check/Time-of-use (TOCTOU) vulnerability in the restore process leading to arbitrary file creation. The issue was fixed with Avast and AVG Antivirus version 22.11	6.5	More Details
CVE-2023-0384	User-controlled operations could have allowed Denial of Service in M-Files Server before 23.4.12528.1 due to uncontrolled memory consumption for a scheduled job.	6.5	More Details
CVE-2023-23892	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Jamie Poitra M Chart plugin <= 1.9.4 versions.	6.5	More Details
CVE-2023-22918	A post-authentication information exposure vulnerability in the CGI program of Zyxel ATP series firmware versions 4.32 through 5.35, USG FLEX series firmware versions 4.50 through 5.35, USG FLEX 50(W) firmware versions 4.16 through 5.35, USG20(W)-VPN firmware versions 4.16 through 5.35, VPN series firmware versions 4.30 through 5.35, NWA110AX firmware version 6.50(ABTG.2) and earlier versions, WAC500 firmware version 6.50(ABVS.0) and earlier versions, and WAX510D firmware version 6.50(ABTF.2) and earlier versions, which could allow a remote authenticated attacker to retrieve encrypted information of the administrator on an affected device.	6.5	More Details
CVE-2023-23838	Directory traversal and file enumeration vulnerability which allowed users to enumerate to different folders of the server.	6.5	More Details
CVE-2023-23832	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in TC Ultimate WP Query Search Filter plugin <= 1.0.10 versions.	6.5	More Details
CVE-2023-1623	The Custom Post Type UI WordPress plugin before 1.13.5 does not properly check for CSRF when sending the debug information to a user supplied email, which could allow attackers to make a logged in admin send such information to an arbitrary email address via a CSRF attack.	6.5	More Details
CVE-2023-1624	The WPCode WordPress plugin before 2.0.9 has a flawed CSRF when deleting log, and does not ensure that the file to be deleted is inside the expected folder. This could allow attackers to make users with the wpcode_activate_snippets capability delete arbitrary log files on the server, including outside of the blog folders	6.5	More Details
CVE-2023-26841	A cross-site request forgery (CSRF) vulnerability in ChurchCRM v4.5.3 allows attackers to change any user's password except for the user that is currently logged in.	6.5	More Details
CVE-2023-26058	An XXE issue was discovered in Nokia NetAct before 22 FP2211 via an XML document to a Performance Manager page. Input validation and a proper XML parser configuration are missing. For an external attacker, it is very difficult to exploit this, because a few dynamically created parameters such as Jsession-id, a CSRF token, and an Nxsrf token would be needed. The attack can realistically only be performed by an internal user.	6.5	More Details
CVE-2023-2239	Exposure of Private Personal Information to an Unauthorized Actor in GitHub repository microweber/microweber prior to 1.3.4.	6.5	More Details
CVE-2023-26057	An XXE issue was discovered in Nokia NetAct before 22 FP2211 via an XML document to the Configuration Dashboard page. Input validation and a proper XML parser configuration are missing. For an external attacker, it is very difficult to exploit this, because a few dynamically created parameters such as Jsession-id, a CSRF token, and an Nxsrf token would be needed. The attack can realistically only be performed by an internal user.	6.5	More Details
CVE-2023-28484	In libxml2 before 2.10.4, parsing of certain invalid XSD schemas can lead to a NULL pointer dereference and subsequently a segfault. This occurs in xmlSchemaFixupComplexType in xmlschemas.c.	6.5	More Details
CVE-2022-44743	Auth. (author+) Stored Cross-Site Scripting (XSS) vulnerability in BlueGlass Jobs for WordPress plugin <= 2.5.11.2 versions.	6.5	More Details
CVE-2023-22698	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in Jason Bobich Theme Blvd Responsive Google Maps plugin <= 1.0.2 versions.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29469	An issue was discovered in libxml2 before 2.10.4. When hashing empty dict strings in a crafted XML document, xmlDictComputeFastKey in dict.c can produce non-deterministic values, leading to various logic and memory errors, such as a double free. This behavior occurs because there is an attempt to use the first byte of an empty string, and any value is possible (not solely the '\0' value).	6.5	More Details
CVE-2023-23717	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in George Gecewicz Portfolio Slideshow plugin <= 1.13.0 versions.	6.5	More Details
CVE-2023-23817	Auth. (contrinbutor+) Cross-Site Scripting (XSS) vulnerability in WebArea	Vera Nedvyzhenko Simple PDF Viewer plugin <= 1.9 versions.	6.5	More Details
CVE-2023-23827	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in Google Maps v3 Shortcode plugin <= 1.2.1 versions.	6.5	More Details
CVE-2023-25620	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when a malicious project file is loaded onto the controller by an authenticated user.	6.5	More Details
CVE-2023-1585	Avast and AVG Antivirus for Windows were susceptible to a Time-of-check/Time-of-use (TOCTOU) vulnerability in the Quarantine process, leading to arbitrary file/directory deletion. The issue was fixed with Avast and AVG Antivirus version 22.11 and virus definitions from 14 February 2023 or later.	6.5	More Details
CVE-2023-2193	Mattermost fails to invalidate existing authorization codes when deauthorizing an OAuth2 app, allowing an attacker possessing an authorization code to generate an access token.	6.5	More Details
CVE-2023-30554	Archery is an open source SQL audit platform. The Archery project contains multiple SQL injection vulnerabilities, that may allow an attacker to query the connected databases. Affected versions are subject to SQL injection in the `sql_api/api_workflow.py` endpoint `ExecuteCheck` which passes unfiltered input to the `explain_check` method in `sql/engines/oracle.py`. User input coming from the `db_name` parameter value in the `api_workflow.py` `ExecuteCheck` endpoint is passed through the `oracle.py` `execute_check` method and to the `explain_check` method for execution. Each of these issues may be mitigated by escaping user input or by using prepared statements when executing SQL queries. This issue is also indexed as `GHSL-2022-103`.	6.5	More Details
CVE-2023-23866	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Carlos Moreira Interactive Geo Maps plugin <= 1.5.8 versions.	6.5	More Details
CVE-2021-38364	An issue was discovered in ONOS 2.5.1. There is an incorrect comparison of flow rules installed by intents. A remote attacker can install or remove a new intent, and consequently modify or delete the existing flow rules related to other intents.	6.5	More Details
CVE-2023-30556	Archery is an open source SQL audit platform. The Archery project contains multiple SQL injection vulnerabilities, that may allow an attacker to query the connected databases. Affected versions are subject to SQL injection in the `optimize_sqltuningadvisor` method of `sql_optimize.py`. User input coming from the `db_name` parameter value in `sql_optimize.py` is passed to the `sqltuningadvisor` method in `oracle.py`for execution. To mitigate escape the variables accepted via user input when used in `sql_optimize.py`. Users may also use prepared statements when dealing with SQL as a mitigation for this issue. This issue is also indexed as `GHSL-2022-107`.	6.5	More Details
CVE-2023-23889	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Fullworks Quick Paypal Payments plugin <= 5.7.25 versions.	6.5	More Details
CVE-2023-2202	Improper Access Control in GitHub repository francoisjacquet/rosariosis prior to 10.9.3.	6.5	More Details
CVE-2022-24109	An issue was discovered in ONOS 2.5.1. To attack an intent installed by a normal user, a remote attacker can install a duplicate intent with a different key, and then remove the duplicate one. This will remove the flow rules of the intent, even though the intent still exists in the controller.	6.5	More Details
CVE-2023-27354	This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of Sonos One Speaker 70.3-35220. Authentication is not required to exploit this vulnerability. The specific flaw exists within the processing of the SMB directory query command. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before reading from memory. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of root. Was ZDI-CAN-19727.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27353	This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of Sonos One Speaker 70.3-35220. Authentication is not required to exploit this vulnerability. The specific flaw exists within the msprox endpoint. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of root. Was ZDI-CAN-19846.	6.5	More Details
CVE-2023-28459	pretalx 2.3.1 before 2.3.2 allows path traversal in HTML export (a non-default feature). Users were able to upload crafted HTML documents that trigger the reading of arbitrary files.	6.5	More Details
CVE-2023-30557	Archery is an open source SQL audit platform. The Archery project contains multiple SQL injection vulnerabilities, that may allow an attacker to query the connected databases. Affected versions are subject to SQL injection in the `data_dictionary.py` `table_info`. User input coming from the `db_name` in and the `tb_name` parameter values in the `sql/data_dictionary.py` `table_info` endpoint is passed to the following methods in the given SQL engine implementations, which concatenate user input unsafely into a SQL query and afterwards pass it to the `query` method of each database engine for execution.The methods are `get_table_meta_data ` in `sql/engines/mssql.py` which passes unsafe user input to the `sql/engines/mssql.py` `query` method, `get_table_desc_data` in `sql/engines/mssql.py`which passes unsafe user input to the `sql/engines/mssql.py` `query`, `get_table_index_data` in `sql/engines/mssql.py`which passes unsafe user input to the `sql/engines/mssql.py` `query` method, `get_table_meta_data` in `sql/engines/oracle.py`which concatenates input which is passed to execution on the database in the `sql/engines/oracle.py` `query` method, `get_table_desc_data` in `sql/engines/oracle.py`which concatenates input which is passed to execution on the database in the `sql/engines/oracle.py` `query` method, and `get_table_index_data` in `sql/engines/oracle.py` which concatenates input which is passed to execution on the database in the `sql/engines/oracle.py` `query` method. Each of these issues may be mitigated by escaping user input or by using prepared statements when executing SQL queries. This issue is also indexed as `GHSL-2022-106`.	6.5	More Details
CVE-2023-30555	Archery is an open source SQL audit platform. The Archery project contains multiple SQL injection vulnerabilities, that may allow an attacker to query the connected databases.Affected versions are subject to SQL injection in the `explain` method in `sql_optimize.py`. User input coming from the `db_name` parameter value in the `explain` endpoint is passed to the following `query` methods of each database engine for execution. `query` in `sql/engines/mssql.py`, and `query` in `sql/engines/oracle.py`. Each of these issues may be mitigated by escaping user input or by using prepared statements when executing SQL queries. This issue is also indexed as `GHSL-2022-108`.	6.5	More Details
CVE-2023-2282	Improper access control in the Web Login listener in Devolutions Remote Desktop Manager 2023.1.22 and earlier on Windows allows an authenticated user to bypass administrator-enforced Web Login restrictions and gain access to entries via an unexpected vector.	6.5	More Details
CVE-2023-30616	Form block is a wordpress plugin designed to make form creation easier. Versions prior to 1.0.2 are subject to a Cross-Site Request Forgery due to a missing nonce check. There is potential for a Cross Site Request Forgery for all form blocks, since it allows to send requests to the forms from any website without a user noticing. Users are advised to upgrade to version 1.0.2. There are no known workarounds for this vulnerability.	6.5	More Details
CVE-2023-30552	Archery is an open source SQL audit platform. The Archery project contains multiple SQL injection vulnerabilities, that may allow an attacker to query the connected databases. Affected versions are subject to SQL injection in the `sql/instance.py` endpoint's `describe` method. In several cases, user input coming from the `tb_name` parameter value, the `db_name` parameter value or the `schema_name` value in the `sql/instance.py` `describe` endpoint is passed to the `describe_table` methods in given SQL engine implementations, which concatenate user input unsafely into a SQL query and afterwards pass it to the `query` method of each database engine for execution. Please take into account that in some cases all three parameter values are concatenated, in other only one or two of them. The affected methods are: `describe_table` in `sql/engines/clickhouse.py`which concatenates input which is passed to execution on the database in the `query` method in `sql/engines/clickhouse.py`, `describe_table` in `sql/engines/mssql.py` which concatenates input which is passed to execution on the database in the `query` methods in `sql/engines/mssql.py`, `describe_table` in `sql/engines/mysql.py`which concatenates input which is passed to execution on the database in the `query` method in `sql/engines/mysql.py`, `describe_table` in `sql/engines/oracle.py` which concatenates input which is passed to execution on the database in the `query` methods in `sql/engines/oracle.py`, `describe_table` in `sql/engines/pgsql.py`which concatenates input which is passed to execution on the database in the `query` methods in `sql/engines/pgsql.py`, `describe_table` in `sql/engines/phoenix.py` which concatenates input which is passed to execution on the database in the `query` method in `sql/engines/phoenix.py`. Each of these issues may be mitigated by escaping user input or by using prepared statements when executing SQL queries. This issue is also indexed as `GHSL-2022-101`.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30553	Archery is an open source SQL audit platform. The Archery project contains multiple SQL injection vulnerabilities, that may allow an attacker to query the connected databases. Affected versions are subject to multiple SQL injections in the `sql_api/api_workflow.py` endpoint `ExecuteCheck`. User input coming from the `db_name` parameter value and the `full_sql` parameter value in the `api_workflow.py` `ExecuteCheck` endpoint is passed to the methods that follow in given SQL engine implementations, which concatenate user input unsafely into a SQL query and afterwards pass it to the `query` method of each database engine for execution. The affected methods are `execute_check` in `sql/engines/clickhouse.py` which concatenates input which is passed to execution on the database in the `sql/engines/clickhouse.py` `query` method, `execute_check` in `sql/engines/goinception.py`which concatenates input which is passed to execution on the database in the `sql/engines/goinception.py` `query` method, `execute_check` in `sql/engines/oracle.py`which passes unsafe user input into the `object_name_check` method in `sql/engines/oracle.py` which in turn is passed to execution on the database in the `sql/engines/oracle.py` `query` method. Each of these issues may be mitigated by escaping user input or by using prepared statements when executing SQL queries. This issue is also indexed as `GHSL-2022-102`.	6.5	More Details
CVE-2022-40723	The PingID RADIUS PCV adapter for PingFederate, which supports RADIUS authentication with PingID MFA, is vulnerable to MFA bypass under certain configurations.	6.5	More Details
CVE-2023-30558	Archery is an open source SQL audit platform. The Archery project contains multiple SQL injection vulnerabilities, that may allow an attacker to query the connected databases. User input coming from the `db_name` in the `sql/data_dictionary.py` `table_list` endpoint is passed to the methods that follow in a given SQL engine implementations, which concatenate user input unsafely into a SQL query and afterwards pass it to the `query` method of each database engine for execution. The affected methods are `get_group_tables_by_db` in `sql/engines/mssql.py`which passes unsafe user input to `sql/engines/mssql.py`, and `get_group_tables_by_db` in `sql/engines/oracle.py`which concatenates input which is passed to execution on the database in the `sql/engines/oracle.py` `query` method. Each of these issues may be mitigated by escaping user input or by using prepared statements when executing SQL queries. This issue is also indexed as `GHSL-2022-105`.	6.5	More Details
CVE-2023-23839	The SolarWinds Platform was susceptible to the Exposure of Sensitive Information Vulnerability. This vulnerability allows users to access Orion.WebCommunityStrings SWIS schema object and obtain sensitive information.	6.5	More Details
CVE-2023-30605	Archery is an open source SQL audit platform. The Archery project contains multiple SQL injection vulnerabilities, that may allow an attacker to query the connected databases. User input coming from the `variable_name` and `variable_value` parameter value in the `sql/instance.py` `param_edit` endpoint is passed to a set of methods in given SQL engine implementations, which concatenate user input unsafely into a SQL query and afterwards pass it to the `query` method of each database engine for execution. The affected methods are: `set_variable` in `sql/engines/goinception.py` which concatenates input which is passed to execution on the database in the `sql/engines/goinception.py`, `get_variables` in `sql/engines/goinception.py` which concatenates input which is passed to execution on the database in the `sql/engines/goinception.py`, `set_variable` in `sql/engines/mysql.py` which concatenates input which is passed to execution on the database in the `sql/engines/mysql.py` `query`, and `get_variables` in `sql/engines/mysql.py`which concatenates input which is passed to execution on the database in the `sql/engines/mysql.py` `query`. Each of these issues may be mitigated by escaping user input or by using prepared statements when executing SQL queries. This advisory is also indexed as `GHSL-2022-104`.	6.5	More Details
CVE-2022-40724	The PingFederate Local Identity Profiles '/pf/idprofile.ping' endpoint is vulnerable to Cross-Site Request Forgery (CSRF) through crafted GET requests.	6.4	More Details
CVE-2023-2214	A vulnerability was found in Campcodes Coffee Shop POS System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/sales/manage_sale.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-226979.	6.3	More Details
CVE-2023-2213	A vulnerability was found in Campcodes Coffee Shop POS System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/products/manage_product.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-226978 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-2218	A vulnerability has been found in SourceCodester Task Reminder System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/user/manage_user.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-226984.	6.3	More Details
CVE-2023-2242	A vulnerability has been found in SourceCodester Online Computer and Laptop Store 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the component GET Parameter Handler. The manipulation of the argument c/s 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-227227.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2212	A vulnerability was found in Campcodes Coffee Shop POS System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/products/view_product.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-226977 was assigned to this vulnerability.	6.3	More Details
CVE-2023-2211	A vulnerability was found in Campcodes Coffee Shop POS System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/categories/manage_category.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-226976.	6.3	More Details
CVE-2023-2210	A vulnerability has been found in Campcodes Coffee Shop POS System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/categories/view_category.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-226975.	6.3	More Details
CVE-2023-2246	A vulnerability has been found in SourceCodester Online Pizza Ordering System 1.0 and classified as critical. This vulnerability affects unknown code of the file admin/ajax.php?action=save_settings. The manipulation of the argument img leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-227236.	6.3	More Details
CVE-2023-2245	A vulnerability was found in hansunCMS 1.4.3. It has been declared as critical. This vulnerability affects unknown code of the file /ueditor/net/controller.ashx?action=catchimage. The manipulation leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-227230 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-2244	A vulnerability was found in SourceCodester Online Eyewear Shop 1.0. It has been classified as critical. This affects an unknown part of the file /admin/orders/update_status.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-227229 was assigned to this vulnerability.	6.3	More Details
CVE-2023-2243	A vulnerability was found in SourceCodester Complaint Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file users/registration.php of the component POST Parameter Handler. The manipulation of the argument fullname leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-227228.	6.3	More Details
CVE-2023-2217	A vulnerability, which was classified as critical, was found in SourceCodester Task Reminder System 1.0. This affects an unknown part of the file /admin/reminders/manage_reminder.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-226983.	6.3	More Details
CVE-2023-2215	A vulnerability classified as critical has been found in Campcodes Coffee Shop POS System 1.0. Affected is an unknown function of the file /admin/user/manage_user.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-226980.	6.3	More Details
CVE-2023-2209	A vulnerability, which was classified as critical, was found in Campcodes Coffee Shop POS System 1.0. Affected is an unknown function of the file /admin/sales/view_details.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-226974 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-2208	A vulnerability, which was classified as critical, has been found in Campcodes Retro Basketball Shoes Online Store 1.0. This issue affects some unknown processing of the file details.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-226973 was assigned to this vulnerability.	6.3	More Details
CVE-2023-2207	A vulnerability classified as critical was found in Campcodes Retro Basketball Shoes Online Store 1.0. This vulnerability affects unknown code of the file contactus1.php. The manipulation of the argument email leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-226972.	6.3	More Details
CVE-2023-2206	A vulnerability classified as critical has been found in Campcodes Retro Basketball Shoes Online Store 1.0. This affects an unknown part of the file contactus.php. The manipulation of the argument email leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-226971.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2205	A vulnerability was found in Campcodes Retro Basketball Shoes Online Store 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /function/login.php. The manipulation of the argument email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-226970 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-2204	A vulnerability was found in Campcodes Retro Basketball Shoes Online Store 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file faqs.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-226969 was assigned to this vulnerability.	6.3	More Details
CVE-2023-20862	In Spring Security, versions 5.7.x prior to 5.7.8, versions 5.8.x prior to 5.8.3, and versions 6.0.x prior to 6.0.3, the logout support does not properly clean the security context if using serialized versions. Additionally, it is not possible to explicitly save an empty security context to the HttpSessionSecurityContextRepository. This vulnerability can keep users authenticated even after they performed logout. Users of affected versions should apply the following mitigation. 5.7.x users should upgrade to 5.7.8. 5.8.x users should upgrade to 5.8.3. 6.0.x users should upgrade to 6.0.3.	6.3	More Details
CVE-2014-125099	A vulnerability has been found in I Recommend This Plugin up to 3.7.2 on WordPress and classified as critical. Affected by this vulnerability is an unknown functionality of the file dot-irecommendthis.php. The manipulation leads to sql injection. The attack can be launched remotely. Upgrading to version 3.7.3 is able to address this issue. The identifier of the patch is 058b3ef5c7577bf557557904a53ecc8599b13649. It is recommended to upgrade the affected component. The identifier VDB-226309 was assigned to this vulnerability.	6.3	More Details
CVE-2022-28354	In the Active Threads Plugin 1.3.0 for MyBB, the activethreads.php date parameter is vulnerable to XSS when setting a time period.	6.1	More Details
CVE-2023-1435	The Ajax Search Pro WordPress plugin before 4.26.2 does not sanitise and escape various parameters before outputting them back in pages, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-26494	lorawan-stack is an open source LoRaWAN network server. Prior to version 3.24.1, an open redirect exists on the login page of the lorawan stack server, allowing an attacker to supply a user controlled redirect upon sign in. This issue may allows malicious actors to phish users, as users assume they were redirected to the homepage on login. Version 3.24.1 contains a fix.	6.1	More Details
CVE-2023-1420	The Ajax Search Lite WordPress plugin before 4.11.1, Ajax Search Pro WordPress plugin before 4.26.2 does not sanitise and escape a parameter before outputting it back in a response of an AJAX action, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2021-44775	Cross-site scripting (XSS) issue in Website app of Odoo Community 15.0 and earlier and Odoo Enterprise 15.0 and earlier, allows remote attackers to inject arbitrary web script in the browser of a victim, by posting crafted contents.	6.1	More Details
CVE-2023-1324	The Easy Forms for Mailchimp WordPress plugin before 6.8.8 does not sanitise and escape some parameters before outputting them back in the response, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-0899	The Steveas WP Live Chat Shoutbox WordPress plugin through 1.4.2 does not sanitise and escape a parameter before outputting it back in the Shoutbox, leading to Stored Cross-Site Scripting which could be used against high privilege users such as admins.	6.1	More Details
CVE-2023-22309	Reflective Cross-Site-Scripting in Webconf in Tribe29 Checkmk Appliance before 1.6.4.	6.1	More Details
CVE-2023-26100	In Progress Flowmon before 12.2.0, an application endpoint failed to sanitize user-supplied input. A threat actor could leverage a reflected XSS vulnerability to execute arbitrary code within the context of a Flowmon user's web browser.	6.1	More Details
CVE-2021-26947	Cross-site scripting (XSS) issue Odoo Community 15.0 and earlier and Odoo Enterprise 15.0 and earlier, allows remote attackers to inject arbitrary web script in the browser of a victim, via a crafted link.	6.1	More Details
CVE-2023-30177	CraftCMS 3.7.59 is vulnerable Cross Site Scripting (XSS). An attacker can inject javascript code into Volume Name.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25314	Cross Site Scripting (XSS) vulnerability in World Wide Broadcast Network AVideo before 12.4, allows attackers to gain sensitive information via the success parameter to /user.	6.1	More Details
CVE-2022-4308	Plaintext Storage of a Password vulnerability in Secomea GateManager (USB wizard) allows Authentication abuse on SiteManager, if the generated file is leaked.	6.1	More Details
CVE-2023-0199	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an out-of-bounds write can lead to denial of service and data tampering.	6.1	More Details
CVE-2021-26263	Cross-site scripting (XSS) issue in Discuss app of Odoo Community 14.0 through 15.0, and Odoo Enterprise 14.0 through 15.0, allows remote attackers to inject arbitrary web script in the browser of a victim, by posting crafted contents.	6.1	More Details
CVE-2023-25346	A reflected cross-site scripting (XSS) vulnerability in ChurchCRM 4.5.3 allows remote attackers to inject arbitrary web script or HTML via the id parameter of /churchcrm/v2/family/not-found.	6.1	More Details
CVE-2023-26599	XSS vulnerability in TripleSign in Tripleplay Platform releases prior to Caveman 3.4.0 allows attackers to inject client-side code to run as an authenticated user via a crafted link.	6.1	More Details
CVE-2022-48150	Shopware v5.5.10 was discovered to contain a cross-site scripting (XSS) vulnerability via the recovery/install/ URI.	6.1	More Details
CVE-2021-44461	Cross-site scripting (XSS) issue in Accounting app of Odoo Enterprise 13.0 through 15.0, allows remote attackers who are able to control the contents of accounting journal entries to inject arbitrary web script in the browser of a victim.	6.1	More Details
CVE-2022-47509	The SolarWinds Platform was susceptible to the Incorrect Input Neutralization Vulnerability. This vulnerability allows a remote adversary with a valid SolarWinds Platform account to append URL parameters to inject HTML.	6.1	More Details
CVE-2021-45071	Cross-site scripting (XSS) issue Odoo Community 15.0 and earlier and Odoo Enterprise 15.0 and earlier, allows remote attackers to inject arbitrary web script in the browser of a victim, via crafted uploaded file names.	6.1	More Details
CVE-2023-20870	VMware Workstation and Fusion contain an out-of-bounds read vulnerability that exists in the functionality for sharing host Bluetooth devices with the virtual machine.	6.0	More Details
CVE-2023-25509	NVIDIA DGX-1 SBIOS contains a vulnerability in Bds, which may lead to code execution, denial of service, and escalation of privileges.	6.0	More Details
CVE-2023-23806	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Davinder Singh Custom Settings plugin <= 1.0 versions.	5.9	More Details
CVE-2023-25485	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Bernhard Kux JSON Content Importer plugin <= 1.3.15 versions.	5.9	More Details
CVE-2022-41612	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Shareaholic Similar Posts plugin <= 3.1.6 versions.	5.9	More Details
CVE-2023-25793	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in George Pattihis Link Juice Keeper plugin <= 2.0.2 versions.	5.9	More Details
CVE-2022-47598	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WP Plugins Pro WP Super Popup plugin <= 1.1.2 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47158	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Pakpobox alfred24 Click & Collect plugin <= 1.1.7 versions.	5.9	More Details
CVE-2023-23938	Tuleap is a Free & Source tool for end to end traceability of application and system developments. Affected versions are subject to a cross site scripting attack which can be injected in the name of a color of select box values of a tracker and then reflected in the tracker administration. Administrative privilege is required, but an attacker with tracker administration rights could use this vulnerability to force a victim to execute uncontrolled code in the context of their browser. This issue has been addressed in Tuleap Community Edition version 14.5.99.4. Users are advised to upgrade. There are no known workarounds for this issue.	5.9	More Details
CVE-2023-1255	Issue summary: The AES-XTS cipher decryption implementation for 64 bit ARM platform contains a bug that could cause it to read past the input buffer, leading to a crash. Impact summary: Applications that use the AES-XTS algorithm on the 64 bit ARM platform can crash in rare circumstances. The AES-XTS algorithm is usually used for disk encryption. The AES-XTS cipher decryption implementation for 64 bit ARM platform will read past the end of the ciphertext buffer if the ciphertext size is 4 mod 5 in 16 byte blocks, e.g. 144 bytes or 1024 bytes. If the memory after the ciphertext buffer is unmapped, this will trigger a crash which results in a denial of service. If an attacker can control the size and location of the ciphertext buffer being decrypted by an application using AES-XTS on 64 bit ARM, the application is affected. This is fairly unlikely making this issue a Low severity one.	5.9	More Details
CVE-2023-25461	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in namithjawahar Wp-Insert plugin <= 2.5.0 versions.	5.9	More Details
CVE-2023-25484	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Oliver Schlöbe Simple Yearly Archive plugin <= 2.1.8 versions.	5.9	More Details
CVE-2023-24386	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Karishma Arora AI Contact Us Form plugin <= 1.0 versions.	5.9	More Details
CVE-2022-47608	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Fullworks Quick Contact Form plugin <= 8.0.3.1 versions.	5.9	More Details
CVE-2023-24005	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Winwar Media Inline Tweet Sharer – Twitter Sharing Plugin plugin <= 2.5.3 versions.	5.9	More Details
CVE-2023-23995	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Tim Reeves & David Stöckl TinyMCE Custom Styles plugin <= 1.1.2 versions.	5.9	More Details
CVE-2022-47435	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Olive Design WP-OliveCart plugin <= 1.1.3 versions.	5.9	More Details
CVE-2022-45361	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Boris Kuzmanov 0mk Shortener plugin <= 0.2 versions.	5.9	More Details
CVE-2023-25490	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Eric Teubert Archivist – Custom Archive Templates plugin <= 1.7.4 versions.	5.9	More Details
CVE-2023-25710	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in DIGITALBLUE Click to Call or Chat Buttons plugin <= 1.4.0 versions.	5.9	More Details
CVE-2023-25451	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPChill CPO Content Types plugin <= 1.1.0 versions.	5.9	More Details
CVE-2023-27425	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in James Irving-Swift Electric Studio Client Login plugin <= 0.8.1 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27614	Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in Ian Haycox Motor Racing League plugin <= 1.9.9 versions.	5.9	More Details
CVE-2023-25479	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Podlove Podlove Subscribe button plugin <= 1.3.7 versions.	5.9	More Details
CVE-2023-23710	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in miniOrange WordPress Social Login and Register (Discord, Google, Twitter, LinkedIn) plugin <= 7.5.14 versions.	5.9	More Details
CVE-2023-23816	Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in Twardes Sitemap Index plugin <= 1.2.3 versions.	5.9	More Details
CVE-2023-1587	Avast and AVG Antivirus for Windows were susceptible to a NULL pointer dereference issue via RPC-interface. The issue was fixed with Avast and AVG Antivirus version 22.11	5.8	More Details
CVE-2023-1998	The Linux kernel allows userspace processes to enable mitigations by calling prctl with PR_SET_SPECULATION_CTRL which disables the speculation feature as well as by using seccomp. We had noticed that on VMs of at least one major cloud provider, the kernel still left the victim process exposed to attacks in some cases even after enabling the spectre-BTI mitigation with prctl. The same behavior can be observed on a bare-metal machine when forcing the mitigation to IBRS on boot command line. This happened because when plain IBRS was enabled (not enhanced IBRS), the kernel had some logic that determined that STIBP was not needed. The IBRS bit implicitly protects against cross-thread branch target injection. However, with legacy IBRS, the IBRS bit was cleared on returning to userspace, due to performance reasons, which disabled the implicit STIBP and left userspace threads vulnerable to cross-thread branch target injection against which STIBP protects.	5.6	More Details
CVE-2023-28084	HPE OneView and HPE OneView Global Dashboard appliance dumps may expose authentication tokens	5.5	More Details
CVE-2023-30408	Jerryscript commit 1a2c047 was discovered to contain a segmentation violation via the component build/bin/jerry.	5.5	More Details
CVE-2023-28086	An HPE OneView appliance dump may expose proxy credential settings	5.5	More Details
CVE-2023-30410	Jerryscript commit 1a2c047 was discovered to contain a stack overflow via the component ecma_op_function_construct at /operations/ecma-function-object.c.	5.5	More Details
CVE-2023-28087	An HPE OneView appliance dump may expose OneView user accounts	5.5	More Details
CVE-2023-30414	Jerryscript commit 1a2c047 was discovered to contain a stack overflow via the component vm_loop at /jerry-core/vm/vm.c.	5.5	More Details
CVE-2023-30406	Jerryscript commit 1a2c047 was discovered to contain a segmentation violation via the component ecma_find_named_property at /base/ecma-helpers.c.	5.5	More Details
CVE-2023-29586	Code Sector TeraCopy 3.9.7 does not perform proper access validation on the source folder during a copy operation. This leads to Arbitrary File Read by allowing any user to copy any directory in the system to a directory they control. NOTE: the Supplier disputes this because only admin users can copy arbitrary folders, and because the 143984 reference is about a different concern (unrelated to directory copying) that was fixed in 3.5b.	5.5	More Details
CVE-2023-28090	An HPE OneView appliance dump may expose SNMPv3 read credentials	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2168	The TaxoPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Suggest Terms Title field in versions up to, and including, 3.6.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with Editor+ permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.5	More Details
CVE-2023-2170	The TaxoPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Related Posts functionality in versions up to, and including, 3.6.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with Editor+ permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.5	More Details
CVE-2023-30402	YASM v1.3.0 was discovered to contain a heap overflow via the function handle_dot_label at /nasm/nasm-token.re. Note: This has been disputed by third parties who argue this is a bug and not a security issue because yasm is a standalone program not designed to run untrusted code.	5.5	More Details
CVE-2023-2169	The TaxoPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Related Posts functionality in versions up to, and including, 3.6.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with Editor+ permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.5	More Details
CVE-2023-30610	aws-sigv4 is a rust library for low level request signing in the aws cloud platform. The `aws_sigv4::SigningParams` struct had a derived `Debug` implementation. When debug-formatted, it would include a user's AWS access key, AWS secret key, and security token in plaintext. When TRACE-level logging is enabled for an SDK, `SigningParams` is printed, thereby revealing those credentials to anyone with access to logs. All users of the AWS SDK for Rust who enabled TRACE-level logging, either globally (e.g. `RUST_LOG=trace`), or for the `aws-sigv4` crate specifically are affected. This issue has been addressed in a set of new releases. Users are advised to upgrade. Users unable to upgrade should disable TRACE-level logging for AWS Rust SDK crates.	5.5	More Details
CVE-2023-29570	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via mjs_ffi_cb_free at src/mjs_ffi.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2023-2166	A null pointer dereference issue was found in can protocol in net/can/af_can.c in the Linux before Linux. ml_priv may not be initialized in the receive path of CAN frames. A local user could use this flaw to crash the system or potentially cause a denial of service.	5.5	More Details
CVE-2023-29579	yasm 1.3.0.55.g101bc was discovered to contain a stack overflow via the component yasm/yasm+0x43b466 in vsprintf. Note: This has been disputed by third parties who argue this is a bug and not a security issue because yasm is a standalone program not designed to run untrusted code.	5.5	More Details
CVE-2023-31081	An issue was discovered in drivers/media/test-drivers/vidtv/vidtv_bridge.c in the Linux kernel 6.2. There is a NULL pointer dereference in vidtv_mux_stop_thread. In vidtv_stop_streaming, after dvb->mux=NULL occurs, it executes vidtv_mux_stop_thread(dvb->mux).	5.5	More Details
CVE-2023-21087	In PreferencesHelper.java, an uncaught exception may cause the device to get stuck in a boot loop. This could lead to local persistent denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261723753	5.5	More Details
CVE-2023-31082	An issue was discovered in drivers/tty/n_gsm.c in the Linux kernel 6.2. There is a sleeping function called from an invalid context in gsmld_write, which will block the kernel. Note: This has been disputed by 3rd parties as not a valid vulnerability.	5.5	More Details
CVE-2023-27652	An issue found in Ego Studio SuperClean v.1.1.9 and v.1.1.5 allows an attacker to gain privileges cause a denial of service via the update_info field of the _default_.xml file.	5.5	More Details
CVE-2023-29583	yasm 1.3.0.55.g101bc was discovered to contain a stack overflow via the function parse_expr5 at /nasm/nasm-parse.c. Note: This has been disputed by third parties who argue this is a bug and not a security issue because yasm is a standalone program not designed to run untrusted code.	5.5	More Details
CVE-2023-29582	yasm 1.3.0.55.g101bc was discovered to contain a stack overflow via the function parse_expr1 at /nasm/nasm-parse.c. Note: This has been disputed by third parties who argue this is a bug and not a security issue because yasm is a standalone program not designed to run untrusted code.	5.5	More Details
CVE-2023-0190	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where a NULL pointer dereference may lead to denial of service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31085	An issue was discovered in drivers/mtd/ubi/cdev.c in the Linux kernel 6.2. There is a divide-by-zero error in do_div(sz,mtd->erasesize), used indirectly by ctrl_cdev_ioctl, when mtd->erasesize is 0.	5.5	More Details
CVE-2021-3429	When instructing cloud-init to set a random password for a new user account, versions before 21.2 would write that password to the world-readable log file /var/log/cloud-init-output.log. This could allow a local user to log in as another user.	5.5	More Details
CVE-2023-31084	An issue was discovered in drivers/media/dvb-core/dvb_frontend.c in the Linux kernel 6.2. There is a blocking operation when a task is in !TASK_RUNNING. In dvb_frontend_get_event, wait_event_interruptible is called; the condition is dvb_frontend_test_event(fepriv,events). In dvb_frontend_test_event, down(&fepriv->sem) is called. However, wait_event_interruptible would put the process to sleep, and down(&fepriv->sem) may block the process.	5.5	More Details
CVE-2023-21091	In canDisplayLocalUi of AppLocalePickerActivity.java, there is a possible way to change system app locales due to a missing permission check. This could lead to local denial of service across user boundaries with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257954050	5.5	More Details
CVE-2023-28328	A NULL pointer dereference flaw was found in the az6027 driver in drivers/media/usb/dev-usb/az6027.c in the Linux Kernel. The message from user space is not checked properly before transferring into the device. This flaw allows a local user to crash the system or potentially cause a denial of service.	5.5	More Details
CVE-2023-28123	A permission misconfiguration in UI Desktop for Windows (Version 0.59.1.71 and earlier) could allow an user to hijack VPN credentials while UID VPN is starting.This vulnerability is fixed in Version 0.62.3 and later.	5.5	More Details
CVE-2023-28327	A NULL pointer dereference flaw was found in the UNIX protocol in net/unix/diag.c In unix_diag_get_exact in the Linux Kernel. The newly allocated skb does not have sk, leading to a NULL pointer. This flaw allows a local user to crash or potentially cause a denial of service.	5.5	More Details
CVE-2023-28124	Improper usage of symmetric encryption in UI Desktop for Windows (Version 0.59.1.71 and earlier) could allow users with access to UI Desktop configuration files to decrypt their content.This vulnerability is fixed in Version 0.62.3 and later.	5.5	More Details
CVE-2023-21082	In getNumberFromCallIntent of NewOutgoingCallIntentBroadcaster.java, there is a possible way to enumerate other user's contact phone number due to a confused deputy. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-257030107	5.5	More Details
CVE-2023-2162	A use-after-free vulnerability was found in iscsi_sw_tcp_session_create in drivers/scsi/iscsi_tcp.c in SCSI sub-component in the Linux Kernel. In this flaw an attacker could leak kernel internal information.	5.5	More Details
CVE-2023-29575	Bento4 v1.6.0-639 was discovered to contain an out-of-memory bug in the mp42aac component.	5.5	More Details
CVE-2023-2177	A null pointer dereference issue was found in the sctp network protocol in net/sctp/stream_sched.c in Linux Kernel. If stream_in allocation is failed, stream_out is freed which would further be accessed. A local user could use this flaw to crash the system or potentially cause a denial of service.	5.5	More Details
CVE-2023-21080	In register_notification_rsp of btif_rc.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-11 Android-12 Android-12L Android-13Android ID: A-245916076	5.5	More Details
CVE-2023-20935	In deserialize of multiple files, 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-11 Android-12 Android-12L Android-13Android ID: A-256589724	5.5	More Details
CVE-2023-20909	In multiple functions of RunningTasks.java, there is a possible privilege escalation due to a missing privilege check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-243130512	5.5	More Details
CVE-2022-2084	Sensitive data could be exposed in world readable logs of cloud-init before version 22.3 when schema failures are reported. This leak could include hashed passwords.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27777	Cross-site scripting (XSS) vulnerability was discovered in Online Jewelry Shop v1.0 that allows attackers to execute arbitrary script via a crafted URL.	5.4	More Details
CVE-2023-22686	Cross-Site Request Forgery (CSRF) vulnerability in TriniTronic Nice PayPal Button Lite plugin <= 1.3.5 versions.	5.4	More Details
CVE-2023-30417	A cross-site scripting (XSS) vulnerability in Pear-Admin-Boot up to v2.0.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Title of a private message.	5.4	More Details
CVE-2023-27776	A stored cross-site scripting (XSS) vulnerability in /index.php?page=category_list of Online Jewelry Shop v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Category Name parameter.	5.4	More Details
CVE-2023-22665	There is insufficient checking of user queries in Apache Jena versions 4.7.0 and earlier, when invoking custom scripts. It allows a remote user to execute arbitrary javascript via a SPARQL query.	5.4	More Details
CVE-2022-45080	Cross-Site Request Forgery (CSRF) vulnerability in KrishaWeb Add Multiple Marker plugin <= 1.2 versions.	5.4	More Details
CVE-2023-26843	A stored Cross-site scripting (XSS) vulnerability in ChurchCRM 4.5.3 allows remote attackers to inject arbitrary web script or HTML via the NoteEditor.php.	5.4	More Details
CVE-2023-27619	Auth (subscriber+) Reflected Cross-Site Scripting (XSS) vulnerability in Macho Themes Regina Lite theme <= 2.0.7 versions.	5.4	More Details
CVE-2023-25759	OS Command Injection in TripleData Reporting Engine in Tripleplay Platform releases prior to Caveman 3.4.0 allows authenticated users to run unprivileged OS level commands via a crafted request payload.	5.4	More Details
CVE-2023-1875	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.12.	5.4	More Details
CVE-2023-25347	A stored cross-site scripting (XSS) vulnerability in ChurchCRM 4.5.3, allows remote attackers to inject arbitrary web script or HTML via input fields. These input fields are located in the "Title" Input Field in EventEditor.php.	5.4	More Details
CVE-2023-0424	The MS-Reviews WordPress plugin through 1.5 does not sanitise and escape reviews, which could allow users any authenticated users, such as Subscribers to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2023-30609	matrix-react-sdk is a react-based SDK for inserting a Matrix chat/VoIP client into a web page. Prior to version 3.71.0, plain text messages containing HTML tags are rendered as HTML in the search results. To exploit this, an attacker needs to trick a user into searching for a specific message containing an HTML injection payload. No cross-site scripting attack is possible due to the hardcoded content security policy. Version 3.71.0 of the SDK patches over the issue. As a workaround, restarting the client will clear the HTML injection.	5.4	More Details
CVE-2023-27090	Cross Site Scripting vulnerability found in TeaCMS storage allows attacker to cause a leak of sensitive information via the article title parameter.	5.4	More Details
CVE-2023-0418	The Video Central for WordPress plugin through 1.3.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2023-0276	The Weaver Xtreme Theme Support WordPress plugin before 6.2.7 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2023-1126	The WP FEvents Book WordPress plugin through 0.46 does not sanitise and escape some parameters, which could allow any authenticated users, such as subscriber to perform Cross-Site Scripting attacks	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2139	A reflected Cross-site Scripting (XSS) Vulnerability in DELMIA Apriso Release 2017 through Release 2022 allows an attacker to execute arbitrary script code.	5.4	More Details
CVE-2023-2118	Insufficient access control in support ticket feature in Devolutions Server 2023.1.5.0 and below allows an authenticated attacker to send support tickets and download diagnostic files via specific endpoints.	5.4	More Details
CVE-2023-25513	NVIDIA CUDA toolkit for Linux and Windows contains a vulnerability in cuobjdump, where an attacker may cause an out-of-bounds read by tricking a user into running cuobjdump on a malformed input file. A successful exploit of this vulnerability may lead to limited denial of service, code execution, and limited information disclosure.	5.3	More Details
CVE-2022-40482	The authentication method in Laravel 8.x through 9.x before 9.32.0 was discovered to be vulnerable to user enumeration via timeless timing attacks with HTTP/2 multiplexing. This is caused by the early return inside the hasValidCredentials method in the Illuminate\Auth\SessionGuard class when a user is found to not exist.	5.3	More Details
CVE-2022-2507	In affected versions of Octopus Deploy it is possible to render user supplied input into the webpage	5.3	More Details
CVE-2021-36436	An issue in Mobicint Backend for Credit Unions v3 allows attackers to retrieve partial email addresses and user entered information via submission to the forgotten-password endpoint.	5.3	More Details
CVE-2023-25512	NVIDIA CUDA toolkit for Linux and Windows contains a vulnerability in cuobjdump, where an attacker may cause an out-of-bounds memory read by running cuobjdump on a malformed input file. A successful exploit of this vulnerability may lead to limited denial of service, code execution, and limited information disclosure.	5.3	More Details
CVE-2023-27495	@fastify/csrf-protection is a plugin which helps protect Fastify servers against CSRF attacks. The CSRF protection enforced by the @fastify/csrf-protection library in combination with @fastify/cookie can be bypassed from network and same-site attackers under certain conditions. @fastify/csrf-protection supports an optional userInfo parameter that binds the CSRF token to the user. This parameter has been introduced to prevent cookie-tossing attacks as a fix for CVE-2021-29624. Whenever userInfo parameter is missing, or its value can be predicted for the target user account, network and same-site attackers can 1. fixate a _csrf cookie in the victim's browser, and 2. forge CSRF tokens that are valid for the victim's session. This allows attackers to bypass the CSRF protection mechanism. As a fix, @fastify/csrf-protection starting from version 6.3.0 (and v4.1.0) includes a server-defined secret hmacKey that cryptographically binds the CSRF token to the value of the _csrf cookie and the userInfo parameter, making tokens non-spoofable by attackers. This protection is effective as long as the userInfo parameter is unique for each user. This is patched in versions 6.3.0 and v4.1.0. Users are advised to upgrade. Users unable to upgrade may use a random, non-predictable userInfo parameter for each user as a mitigation.	5.3	More Details
CVE-2022-29609	An issue was discovered in ONOS 2.5.1. An intent with the same source and destination shows the INSTALLING state, indicating that its flow rules are installing. Improper handling of such an intent is misleading to a network operator.	5.3	More Details
CVE-2023-25514	NVIDIA CUDA toolkit for Linux and Windows contains a vulnerability in cuobjdump, where an attacker may cause an out-of-bounds read by tricking a user into running cuobjdump on a malformed input file. A successful exploit of this vulnerability may lead to limited denial of service, code execution, and limited information disclosure.	5.3	More Details
CVE-2023-26840	A cross-site request forgery (CSRF) vulnerability in ChurchCRM v4.5.3 allows attackers to set a person to a user and set that user to be an Administrator.	5.3	More Details
CVE-2023-2241	A vulnerability, which was classified as critical, was found in PoDoFo 0.10.0. Affected is the function readXRefStreamEntry of the file PdfXRefStreamParserObject.cpp. The manipulation leads to heap-based buffer overflow. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The patch is identified as 535a786f124b739e3c857529cecc29e4eeb79778. It is recommended to apply a patch to fix this issue. VDB-227226 is the identifier assigned to this vulnerability.	5.3	More Details
CVE-2022-29944	An issue was discovered in ONOS 2.5.1. There is an incorrect comparison of paths installed by intents. An existing intents does not redirect to a new path, even if a new intent that shares the path with higher priority is installed.	5.3	More Details
CVE-2023-29922	PowerJob V4.3.1 is vulnerable to Incorrect Access Control via the create user/save interface.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27043	The email module of Python through 3.11.3 incorrectly parses e-mail addresses that contain a special character. The wrong portion of an RFC2822 header is identified as the value of the addr-spec. In some applications, an attacker can bypass a protection mechanism in which application access is granted only after verifying receipt of e-mail to a specific domain (e.g., only @company.example.com addresses may be used for signup). This occurs in email/_parseaddr.py in recent versions of Python.	5.3	More Details
CVE-2023-29923	PowerJob V4.3.1 is vulnerable to Insecure Permissions. via the list job interface.	5.3	More Details
CVE-2023-29921	PowerJob V4.3.1 is vulnerable to Incorrect Access Control via the create app interface.	5.3	More Details
CVE-2023-30458	A username enumeration issue was discovered in Medicine Tracker System 1.0. The login functionality allows a malicious user to guess a valid username due to a different response time from invalid usernames. When one enters a valid username, the response time increases depending on the length of the supplied password.	5.3	More Details
CVE-2023-29479	Ribose RNP before 0.16.3 may hang when the input is malformed.	5.3	More Details
CVE-2023-21090	In parseUsesPermission of ParsingPackageUtils.java, there is a possible boot loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-259942609	5.0	More Details
CVE-2023-29513	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. If guest has view right on any document. It's possible to create a new user using the `distribution/firstadminuser.wiki` in the wrong context. This vulnerability has been patched in XWiki 15.0-rc-1 and 14.10.1. There is no known workaround other than upgrading.	5.0	More Details
CVE-2023-0203	NVIDIA ConnectX-5, ConnectX-6, and ConnectX6-DX contain a vulnerability in the NIC firmware, where an unprivileged user can exploit insufficient granularity of access control, which may lead to denial of service.	5.0	More Details
CVE-2023-0205	NVIDIA ConnectX-5, ConnectX-6, and ConnectX6-DX contain a vulnerability in the NIC firmware, where an unprivileged user can exploit insufficient granularity of access control, which may lead to denial of service.	5.0	More Details
CVE-2023-29910	H3C Magic R200 version R200V100R004 was discovered to contain a stack overflow via the UpdateMacClone interface at /goform/aspForm.	4.9	More Details
CVE-2023-29911	H3C Magic R200 version R200V100R004 was discovered to contain a stack overflow via the AddMacList interface at /goform/aspForm.	4.9	More Details
CVE-2023-29912	H3C Magic R200 R200V100R004 was discovered to contain a stack overflow via the DelvsList interface at /goform/aspForm.	4.9	More Details
CVE-2023-29909	H3C Magic R200 version R200V100R004 was discovered to contain a stack overflow via the AddWlanMacList interface at /goform/aspForm.	4.9	More Details
CVE-2023-29913	H3C Magic R200 version R200V100R004 was discovered to contain a stack overflow via the SetAPWifiorLedInfoById interface at /goform/aspForm.	4.9	More Details
CVE-2023-29914	H3C Magic R200 version R200V100R004 was discovered to contain a stack overflow via the DeltriggerList interface at /goform/aspForm.	4.9	More Details
CVE-2023-29908	H3C Magic R200 version R200V100R004 was discovered to contain a stack overflow via the SetMobileAPInfoById interface at /goform/aspForm.	4.9	More Details
CVE-2023-29915	H3C Magic R200 version R200V100R004 was discovered to contain a stack overflow via CMD parameter at /goform/aspForm.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29917	H3C Magic R200 version R200V100R004 was discovered to contain a stack overflow via go parameter at /goform/aspForm.	4.9	More Details
CVE-2023-29907	H3C Magic R200 version R200V100R004 was discovered to contain a stack overflow via the Edit_BasicSSID_5G interface at /goform/aspForm.	4.9	More Details
CVE-2023-29906	H3C Magic R200 version R200V100R004 was discovered to contain a stack overflow via the Edit_BasicSSID interface at /goform/aspForm.	4.9	More Details
CVE-2023-22894	Strapi through 4.5.5 allows attackers (with access to the admin panel) to discover sensitive user details by exploiting the query filter. The attacker can filter users by columns that contain sensitive information and infer a value from API responses. If the attacker has super admin access, then this can be exploited to discover the password hash and password reset token of all users. If the attacker has admin panel access to an account with permission to access the username and email of API users with a lower privileged role (e.g., Editor or Author), then this can be exploited to discover sensitive information for all API users but not other admin accounts.	4.9	More Details
CVE-2023-29905	H3C Magic R200 version R200V100R004 was discovered to contain a stack overflow via the UpdateSnat interface at /goform/aspForm.	4.9	More Details
CVE-2023-0317	Unprotected Alternate Channel vulnerability in debug console of GateManager allows system administrator to obtain sensitive information.	4.9	More Details
CVE-2023-29916	H3C Magic R200 version R200V100R004 was discovered to contain a stack overflow via the UpdateWanParams interface at /goform/aspForm.	4.9	More Details
CVE-2023-30776	An authenticated user with specific data permissions could access database connections stored passwords by requesting a specific REST API. This issue affects Apache Superset version 1.3.0 up to 2.0.1.	4.9	More Details
CVE-2023-31045	A stored Cross-site scripting (XSS) issue in Text Editors and Formats in Backdrop CMS before 1.24.2 allows remote attackers to inject arbitrary web script or HTML via the name parameter. When a user is editing any content type (e.g., page, post, or card) as an admin, the stored XSS payload is executed upon selecting a malicious text formatting option. NOTE: the vendor disputes the security relevance of this finding because "any administrator that can configure a text format could easily allow Full HTML anywhere."	4.8	More Details
CVE-2023-0420	The Custom Post Type and Taxonomy GUI Manager WordPress plugin through 1.1 does not have CSRF, and is lacking sanitising as well as escaping in some parameters, allowing attackers to make a logged in admin put Stored Cross-Site Scripting payloads via CSRF	4.8	More Details
CVE-2023-27990	The cross-site scripting (XSS) vulnerability in Zyxel ATP series firmware versions 4.32 through 5.35, USG FLEX series firmware versions 4.50 through 5.35, USG FLEX 50(W) firmware versions 4.16 through 5.35, USG20(W)-VPN firmware versions 4.16 through 5.35, and VPN series firmware versions 4.30 through 5.35, which could allow an authenticated attacker with administrator privileges to store malicious scripts in a vulnerable device. A successful XSS attack could then result in the stored malicious scripts being executed when the user visits the Logs page of the GUI on the device.	4.8	More Details
CVE-2022-44582	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Apptivo Apptivo Business Site CRM plugin <= 3.0.12 versions.	4.8	More Details
CVE-2022-44631	Auth. (author+) Stored Cross-Site Scripting (XSS) vulnerability in 1app Technologies, Inc 1app Business Forms plugin <= 1.0.0 versions.	4.8	More Details
CVE-2022-44594	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Codebangers All in One Time Clock Lite plugin <= 1.3.320 versions.	4.8	More Details
CVE-2023-29848	Bang Resto 1.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the itemName parameter in the admin/menu.php Add New Menu function.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2191	Cross-site Scripting (XSS) - Stored in GitHub repository azuracast/azuracast prior to 0.18.	4.8	More Details
CVE-2023-0045	The current implementation of the prctl syscall does not issue an IBPB immediately during the syscall. The ib_prctl_set function updates the Thread Information Flags (TIFs) for the task and updates the SPEC_CTRL MSR on the function __speculation_ctrl_update, but the IBPB is only issued on the next schedule, when the TIF bits are checked. This leaves the victim vulnerable to values already injected on the BTB, prior to the prctl syscall. The patch that added the support for the conditional mitigation via prctl (ib_prctl_set) dates back to the kernel 4.9.176. We recommend upgrading past commit a664ec9158eeddd75121d39c9a0758016097fa96	4.7	More Details
CVE-2023-1382	A data race flaw was found in the Linux kernel, between where con is allocated and con->sock is set. This issue leads to a NULL pointer dereference when accessing con->sock->sk in net/tipc/topsrv.c in the tipc protocol in the Linux kernel.	4.7	More Details
CVE-2023-31083	An issue was discovered in drivers/bluetooth/hci_ldisc.c in the Linux kernel 6.2. In hci_uart_tty_ioctl, there is a race condition between HCIUARTSETPROTO and HCIUARTGETPROTO. HCI_UART_PROTO_SET is set before hu->proto is set. A NULL pointer dereference may occur.	4.7	More Details
CVE-2023-2019	A flaw was found in the Linux kernel's netdevsim device driver, within the scheduling of events. This issue results from the improper management of a reference count. This may allow an attacker to create a denial of service condition on the system.	4.4	More Details
CVE-2023-26099	An issue was discovered in Telindus Apsal 3.14.2022.235 b. The consultation permission is insecure.	4.4	More Details
CVE-2023-2269	A denial of service problem was found, due to a possible recursive locking scenario, resulting in a deadlock in table_clear in drivers/md/dm-ioctl.c in the Linux Kernel Device Mapper-Multipathing sub-component.	4.4	More Details
CVE-2021-44465	Improper access control in Odoo Community 13.0 and earlier and Odoo Enterprise 13.0 and earlier allows authenticated attackers to subscribe to receive future notifications and comments related to arbitrary business records in the system, via crafted RPC requests.	4.3	More Details
CVE-2023-30611	Discourse-reactions is a plugin that allows user to add their reactions to the post in the Discourse messaging platform. In affected versions data about what reactions were performed on a post in a private topic could be leaked. This issue has been addressed in version 0.3. Users are advised to upgrade. Users unable to upgrade should disable the discourse-reactions plugin to fully mitigate the issue.	4.3	More Details
CVE-2023-29200	Contao is an open source content management system. Prior to versions 4.9.40, 4.13.21, and 5.1.4, logged in users can list arbitrary system files in the file manager by manipulating the Ajax request. However, it is not possible to read the contents of these files. Users should update to Contao 4.9.40, 4.13.21 or 5.1.4 to receive a patch. There are no known workarounds.	4.3	More Details
CVE-2023-29520	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. It's possible to break many translations coming from wiki pages by creating a corrupted document containing a translation object. This will lead to a broken page. The vulnerability has been patched in XWiki 15.0-rc-1, 14.10.1, 14.4.8, and 13.10.11. Users are advised to upgrade. There are no workarounds other than fixing any way to create a document that fail to load.	4.3	More Details
CVE-2023-26839	A cross-site request forgery (CSRF) vulnerability in ChurchCRM v4.5.3 allows attackers to edit information for existing people on the site.	4.3	More Details
CVE-2022-45074	Cross-Site Request Forgery (CSRF) vulnerability in Paramveer Singh for Arete IT Private Limited Activity Reactions For Buddypress plugin <= 1.0.22 versions.	4.3	More Details
CVE-2023-23879	Cross-Site Request Forgery (CSRF) vulnerability in Nicolas Zeh PHP Execution plugin <= 1.0.0 versions.	4.3	More Details
CVE-2023-1414	The WP VR WordPress plugin before 8.3.0 does not have authorisation and CSRF checks in various AJAX actions, one in particular could allow any authenticated users, such as subscriber to update arbitrary tours	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25601	On version 3.0.0 through 3.1.1, Apache DolphinScheduler's python gateway suffered from improper authentication: an attacker could use a socket bytes attack without authentication. This issue has been fixed from version 3.1.2 onwards. For users who use version 3.0.0 to 3.1.1, you can turn off the python-gateway function by changing the value `python-gateway.enabled=false` in configuration file `application.yaml`. If you are using the python gateway, please upgrade to version 3.1.2 or above.	4.3	More Details
CVE-2022-4944	A vulnerability, which was classified as problematic, has been found in kalcaddle KodExplorer up to 4.49. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 4.50 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-227000.	4.3	More Details
CVE-2023-1767	The Snyk Advisor website (https://snyk.io/advisor/) was vulnerable to a stored XSS prior to 28th March 2023. A feature of Snyk Advisor is to display the contents of a scanned package's Readme on its package health page. An attacker could create a package in NPM with an associated markdown README file containing XSS-able HTML tags. Upon Snyk Advisor importing the package, the XSS would run each time an end user browsed to the package's page on Snyk Advisor.	4.3	More Details
CVE-2023-28458	pretalx 2.3.1 before 2.3.2 allows path traversal in HTML export (a non-default feature). Organizers can trigger the overwriting (with the standard pretalx 404 page content) of an arbitrary file.	4.3	More Details
CVE-2022-48477	In JetBrains Hub before 2023.1.15725 SSRF protection in Auth Module integration was missing	4.1	More Details
CVE-2023-30612	Cloud hypervisor is a Virtual Machine Monitor for Cloud workloads. This vulnerability allows users to close arbitrary open file descriptors in the Cloud Hypervisor process via sending malicious HTTP request through the HTTP API socket. As a result, the Cloud Hypervisor process can be easily crashed, causing Deny-of-Service (DoS). This can also be a potential Use-After-Free (UAF) vulnerability. Users require to have the write access to the API socket file to trigger this vulnerability. Impacted versions of Cloud Hypervisor include upstream main branch, v31.0, and v30.0. The vulnerability was initially detected by our `http_api_fuzzer` via oss-fuzz. This issue has been addressed in versions 30.1 and 31.1. Users unable to upgrade may mitigate this issue by ensuring the write access to the API socket file is granted to trusted users only.	4.0	More Details
CVE-2023-30544	Kiwi TCMS is an open source test management system. In versions of Kiwi TCMS prior to 12.2, users were able to update their email addresses via the `My profile` admin page. This page allowed them to change the email address registered with their account without the ownership verification performed during account registration. Operators of Kiwi TCMS should upgrade to v12.2 or later to receive a patch. No known workarounds exist.	3.9	More Details
CVE-2022-23721	PingID integration for Windows login prior to 2.9 does not handle duplicate usernames, which can lead to a username collision when two people with the same username are provisioned onto the same machine at different times.	3.8	More Details
CVE-2023-2112	Desktop component service allows lateral movement between sessions in M-Files before 23.4.12455.0.	3.6	More Details
CVE-2012-10014	A vulnerability classified as problematic has been found in Kau-Boy Backend Localization Plugin 2.0 on WordPress. Affected is the function backend_localization_admin_settings/backend_localization_save_setting/backend_localization_login_form/localize_backend of the file backend_localization.php. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 2.0.1 is able to address this issue. The name of the patch is 36f457ee16dd114e510fd91a3ea9fbb3c1f87184. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-227232.	3.5	More Details
CVE-2012-10013	A vulnerability was found in Kau-Boy Backend Localization Plugin up to 1.6.1 on WordPress. It has been rated as problematic. This issue affects some unknown processing of the file backend_localization.php. The manipulation leads to cross site scripting. The attack may be initiated remotely. Upgrading to version 2.0 is able to address this issue. The patch is named 43dc96defd7944da12ff116476a6890acd7dd24b. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-227231.	3.5	More Details
CVE-2023-2216	A vulnerability classified as problematic was found in Campcodes Coffee Shop POS System 1.0. Affected by this vulnerability is an unknown functionality of the file /classes/Users.php. The manipulation of the argument firstname leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-226981 was assigned to this vulnerability.	3.5	More Details
CVE-2023-2219	A vulnerability was found in SourceCodester Task Reminder System 1.0 and classified as problematic. This issue affects some unknown processing of the file /classes/Users.php. The manipulation of the argument id leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-226985 was assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2220	A vulnerability was found in Dream Technology mica up to 3.0.5. It has been classified as problematic. Affected is an unknown function of the component Form Object Handler. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. VDB-226986 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2022-4942	A vulnerability was found in mportuga eslint-detailed-reporter up to 0.9.0 and classified as problematic. Affected by this issue is the function renderIssue in the library lib/template-generator.js. The manipulation of the argument message leads to cross site scripting. The attack may be launched remotely. The patch is identified as 505c190efd4905990db6207863bdcbd9b1d7e1bd. It is recommended to apply a patch to fix this issue. VDB-226310 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-2226	Due to insufficient validation in the PE and OLE parsers in Rapid7's Velociraptor versions earlier than 0.6.8 allows attacker to crash Velociraptor during parsing of maliciously malformed files. For this attack to succeed, the attacker needs to be able to introduce malicious files to the system at the same time that Velociraptor attempts to collect any artifacts that attempt to parse PE files, Authenticode signatures, or OLE files. After crashing, the Velociraptor service will restart and it will still be possible to collect other artifacts.	3.3	More Details
CVE-2023-25510	NVIDIA CUDA Toolkit SDK for Linux and Windows contains a NULL pointer dereference in cuobjdump, where a local user running the tool against a malformed binary may cause a limited denial of service.	3.3	More Details
CVE-2023-22846	Datakit CrossCadWare_x64.dll contains an out-of-bounds read past the end of an allocated buffer while parsing a specially crafted SLDPRT file. This vulnerability could allow an attacker to disclose sensitive information.	3.3	More Details
CVE-2023-22354	Datakit CrossCadWare_x64.dll contains an out-of-bounds read past the end of an allocated buffer while parsing a specially crafted SLDPRT file. This vulnerability could allow an attacker to disclose sensitive information.	3.3	More Details
CVE-2023-22321	Datakit CrossCadWare_x64.dll contains an out-of-bounds read past the end of an allocated buffer while parsing a specially crafted SLDPRT file. This vulnerability could allow an attacker to disclose sensitive information.	3.3	More Details
CVE-2023-22295	Datakit CrossCadWare_x64.dll contains an out of bounds read past the end of an allocated buffer while parsing a specially crafted SLDPRT file. This vulnerability could allow an attacker to disclose sensitive information.	3.3	More Details
CVE-2023-25815	In Git for Windows, the Windows port of Git, no localized messages are shipped with the installer. As a consequence, Git is expected not to localize messages at all, and skips the gettext initialization. However, due to a change in MINGW-packages, the `gettext()` function's implicit initialization no longer uses the runtime prefix but uses the hard-coded path `C:\mingw64\share\locale` to look for localized messages. And since any authenticated user has the permission to create folders in `C:\` (and since `C:\mingw64` does not typically exist), it is possible for low-privilege users to place fake messages in that location where `git.exe` will pick them up in version 2.40.1. This vulnerability is relatively hard to exploit and requires social engineering. For example, a legitimate message at the end of a clone could be maliciously modified to ask the user to direct their web browser to a malicious website, and the user might think that the message comes from Git and is legitimate. It does require local write access by the attacker, though, which makes this attack vector less likely. Version 2.40.1 contains a patch for this issue. Some workarounds are available. Do not work on a Windows machine with shared accounts, or alternatively create a `C:\mingw64` folder and leave it empty. Users who have administrative rights may remove the permission to create folders in `C:\`.	3.3	More Details
CVE-2023-25511	NVIDIA CUDA Toolkit for Linux and Windows contains a vulnerability in cuobjdump, where a division-by-zero error may enable a user to cause a crash, which may lead to a limited denial of service.	3.3	More Details
CVE-2023-30618	Kitchen-Terraform provides a set of Test Kitchen plugins which enable the use of Test Kitchen to converge a Terraform configuration and verify the resulting infrastructure systems with InSpec controls. Kitchen-Terraform v7.0.0 introduced a regression which caused all Terraform output values, including sensitive values, to be printed at the `info` logging level during the `kitchen converge` action. Prior to v7.0.0, the output values were printed at the `debug` level to avoid writing sensitive values to the terminal by default. An attacker would need access to the local machine in order to gain access to these logs during an operation. Users are advised to upgrade. There are no known workarounds for this vulnerability.	3.2	More Details
CVE-2023-28847	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform. In Nextcloud Server 24.0.0 prior to 24.0.11 and 25.0.0 prior to 25.0.5; as well as Nextcloud Server Enterprise 23.0.0 prior to 23.0.12.6, 24.0.0 prior to 24.0.11, and 25.0.0 prior to 25.0.5; an attacker is not restricted in verifying passwords of share links so they can just start brute forcing the password. Nextcloud Server 24.0.11 and 25.0.5 and Nextcloud Enterprise Server 23.0.12.6, 24.0.11, and 25.0.5 contain a fix for this issue. No known workarounds are available.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2281	When archiving a team, Mattermost fails to sanitize the related Websocket event sent to currently connected clients. This allows the clients to see the name, display name, description, and other data about the archived team.	3.1	More Details
CVE-2022-38125	Improper Restriction of Communication Channel to Intended Endpoints vulnerability in Secomea SiteManager (FTP Agent modules) allows Exploiting Trust in Client.	2.9	More Details
CVE-2023-2293	A vulnerability was found in SourceCodester Purchase Order Management System 1.0. It has been classified as problematic. This affects an unknown part of the file classes/Master.php?f=save_item. The manipulation of the argument description with the input <script>alert(document.cookie)</script> leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-227463.	2.4	More Details
CVE-2023-30842	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-25313. Reason: This candidate is a reservation duplicate of CVE-2023-25313. Notes: All CVE users should reference CVE-2023-25313 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-27752	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-27751	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