SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 01 November 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-2023-46604	The Java OpenWire protocol marshaller is vulnerable to Remote Code Execution. This vulnerability may allow a remote attacker with network access to either a Java-based OpenWire broker or client to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause either the client or the broker (respectively) to instantiate any class on the classpath. Users are recommended to upgrade both brokers and clients to version 5.15.16, 5.16.7, 5.17.6, or 5.18.3 which fixes this issue.	10.0	More Details
CVE-2023-40050	Upload profile either through API or user interface in Chef Automate prior to and including version 4.10.29 using InSpec check command with maliciously crafted profile allows remote code execution.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37913	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Starting in version 3.5-milestone-1 and prior to versions 14.10.8 and 15.3-rc-1, triggering the office converter with a specially crafted file name allows writing the attachment's content to an attacker-controlled location on the server as long as the Java process has write access to that location. In particular in the combination with attachment moving, a feature introduced in XWiki 14.0, this is easy to reproduce but it also possible to reproduce in versions as old as XWiki 3.5 by uploading the attachment through the REST API which doesn't remove `/` or `\` from the filename. As the mime type of the attachment doesn't matter for the exploitation, this could e.g., be used to replace the `jar`-file of an extension which would allow executing arbitrary Java code and thus impact the confidentiality, integrity and availability of the XWiki installation. This vulnerability has been patched in XWiki 14.10.8 and 15.3RC1. There are no known workarounds apart from disabling the office converter.	9.9	More Details
CVE-2023-37912	XWiki Rendering is a generic Rendering system that converts textual input in a given syntax into another syntax. Prior to version 14.10.6 of `org.xwiki.platform:xwiki-core-rendering-macro-footnotes` and `org.xwiki.platform:xwiki-rendering-macro-footnotes` and prior to version 15.1-rc-1 of `org.xwiki.platform:xwiki-rendering-macro-footnotes`, the footnote macro executed its content in a potentially different context than the one in which it was defined. In particular in combination with the include macro, this allows privilege escalation from a simple user account in XWiki to programming rights and thus remote code execution, impacting the confidentiality, integrity and availability of the whole XWiki installation. This vulnerability has been patched in XWiki 14.10.6 and 15.1-rc-1. There is no workaround apart from upgrading to a fixed version of the footnote macro.	9.9	More Details
CVE-2023-5199	The PHP to Page plugin for WordPress is vulnerable Local File Inclusion to Remote Code Execution in versions up to, and including, 0.3 via the 'php-to-page' shortcode. This allows authenticated attackers with subscriber-level permissions or above, to include local file and potentially execute code on the server. While subscribers may need to poison log files or otherwise get a file installed in order to achieve remote code execution, author and above users can upload files by default and achieve remote code execution easily.	9.9	More Details
CVE-2023-37909	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Starting in version 5.1-rc-1 and prior to versions 14.10.8 and 15.3-rc-1, 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. This has been patched in XWiki 14.10.8 and 15.3-rc-1 by adding proper escaping. As a workaround, the patch can be manually applied to the document `Menu.UIExtensionSheet`; only three lines need to be changed.	9.9	More Details
CVE-2023-46665	Sielco PolyEco1000 is vulnerable to an authentication bypass vulnerability due to an attacker modifying passwords in a POST request and gain unauthorized access to the affected device with administrative privileges.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46435	Sourcecodester Packers and Movers Management System v1.0 is vulnerable to SQL Injection via mpms/?p=services/view_service&id.	9.8	More Details
CVE-2023-44267	Online Art Gallery v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'lnm' parameter of the header.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-46661	Sielco PolyEco1000 is vulnerable to an attacker escalating their privileges by modifying passwords in POST requests.	9.8	More Details
CVE-2023-39726	An issue in Mintty v.3.6.4 and before allows a remote attacker to execute arbitrary code via crafted commands to the terminal.	9.8	More Details
CVE-2018-17558	Hardcoded manufacturer credentials and an OS command injection vulnerability in the /cgi-bin/mft/ directory on ABUS TVIP TVIP20050 LM.1.6.18, TVIP10051 LM.1.6.18, TVIP11050 MG.1.6.03.05, TVIP20550 LM.1.6.18, TVIP10050 LM.1.6.18, TVIP11550 MG.1.6.03, TVIP21050 MG.1.6.03, and TVIP51550 MG.1.6.03 cameras allow remote attackers to execute code as root.	9.8	More Details
CVE-2023-46747	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	9.8	More Details
CVE-2023-42769	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter.	9.8	More Details
CVE-2018-17878	Buffer Overflow vulnerability in certain ABUS TVIP cameras allows attackers to gain control of the program via crafted string sent to sprintf() function.	9.8	More Details
CVE-2018-17879	An issue was discovered on certain ABUS TVIP cameras. The CGI scripts allow remote attackers to execute code via system() as root. There are several injection points in various scripts.	9.8	More Details
CVE-2023-42406	SQL injection vulnerability in D-Link Online behavior audit gateway DAR-7000 V31R02B1413C allows a remote attacker to obtain sensitive information and execute arbitrary code via the editrole.php component.	9.8	More Details
CVE-2023-45498	VinChin Backup & Recovery v5.0.*, v6.0.*, v6.7.*, and v7.0.* was discovered to contain a command injection vulnerability.	9.8	More Details
CVE-2023-45499	VinChin Backup & Recovery v5.0.*, v6.0.*, v6.7.*, and v7.0.* was discovered to contain hardcoded credentials.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5807	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in TRtek Software Education Portal allows SQL Injection.This issue affects Education Portal: before 3.2023.29.	9.8	More Details
CVE-2023-43208	NextGen Healthcare Mirth Connect before version 4.4.1 is vulnerable to unauthenticated remote code execution. Note that this vulnerability is caused by the incomplete patch of CVE-2023-37679.	9.8	More Details
CVE-2023-26568	Unauthenticated SQL injection in the GetStudentGroupStudents method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers.	9.8	More Details
CVE-2023-30967	Gotham Orbital-Simulator service prior to 0.692.0 was found to be vulnerable to a Path traversal issue allowing an unauthenticated user to read arbitrary files on the file system.	9.8	More Details
CVE-2023-46853	In Memcached before 1.6.22, an off-by-one error exists when processing proxy requests in proxy mode, if \n is used instead of \r\n.	9.8	More Details
CVE-2023-46424	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_422BD4 function.	9.8	More Details
CVE-2023-46423	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_417094 function.	9.8	More Details
CVE-2023-46422	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_411994 function.	9.8	More Details
CVE-2023-46421	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_411D00 function.	9.8	More Details
CVE-2023-46420	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_41590C function.	9.8	More Details
CVE-2023-46419	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_415730 function.	9.8	More Details
CVE-2023-46418	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_412688 function.	9.8	More Details
CVE-2023-46417	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_415498 function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46416	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_ The 41A414 function.	9.8	More Details
CVE-2023-46415	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_41E588 function.	9.8	More Details
CVE-2023-46414	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_ 41D494 function.	9.8	More Details
CVE-2023-26569	Unauthenticated SQL injection in the StudentPopupDetails_Timetable method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers.	9.8	More Details
CVE-2023-46412	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a command execution vulnerability via the sub_41D998 function.	9.8	More Details
CVE-2023-46584	SQL Injection vulnerability in PHPGurukul Nipah virus (NiV) " Testing Management System v.1.0 allows a remote attacker to escalate privileges via a crafted request to the new-user-testing.php endpoint.	9.8	More Details
CVE-2023-46569	An out-of-bounds read in radare2 v.5.8.9 and before exists in the print_insn32_fpu function of libr/arch/p/nds32/nds32-dis.h.	9.8	More Details
CVE-2023-46509	An issue in Contec SolarView Compact v.6.0 and before allows an attacker to execute arbitrary code via the texteditor.php component.	9.8	More Details
CVE-2023-24000	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in GamiPress gamipress allows SQL Injection.This issue affects GamiPress: from n/a through 2.5.7.	9.8	More Details
CVE-2023-46484	An issue in TOTOlink X6000R V9.4.0cu.852_B20230719 allows a remote attacker to execute arbitrary code via the setLedCfg function.	9.8	More Details
CVE-2023-46993	In TOTOLINK A3300R V17.0.0cu.557_B20221024 when dealing with setLedCfg request, there is no verification for the enable parameter, which can lead to command injection.	9.8	More Details
CVE-2023-42425	An issue in Turing Video Turing Edge+ EVC5FD v.1.38.6 allows remote attacker to execute arbitrary code and obtain sensitive information via the cloud connection components.	9.8	More Details
CVE-2023-37966	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Solwin Infotech User Activity Log user-activity-log allows SQL Injection.This issue affects User Activity Log: from n/a through 1.6.2.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36508	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in BestWebSoft Contact Form to DB by BestWebSoft – Messages Database Plugin For WordPress contact-form-to-db allows SQL Injection.This issue affects Contact Form to DB by BestWebSoft – Messages Database Plugin For WordPress: from n/a through 1.7.1.	9.8	More Details
CVE-2023-35879	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WooCommerce Product Vendors allows SQL Injection.This issue affects Product Vendors: from n/a through 2.1.78.	9.8	More Details
CVE-2023-33927	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Themeisle Multiple Page Generator Plugin – MPG multiple-pages-generator-by-porthas allows SQL Injection.This issue affects Multiple Page Generator Plugin – MPG: from n/a through 3.3.19.	9.8	More Details
CVE-2023-31212	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CRM Perks Database for Contact Form 7, WPforms, Elementor forms contact-form-entries allows SQL Injection.This issue affects Database for Contact Form 7, WPforms, Elementor forms: from n/a through 1.3.0.	9.8	More Details
CVE-2023-24410	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Contact Form - WPManageNinja LLC Contact Form Plugin – Fastest Contact Form Builder Plugin for WordPress by Fluent Forms fluentform allows SQL Injection.This issue affects Contact Form Plugin – Fastest Contact Form Builder Plugin for WordPress by Fluent Forms: from n/a through 4.3.25.	9.8	More Details
CVE-2023-22518	All versions of Confluence Data Center and Server are affected by this unexploited vulnerability. This Improper Authorization vulnerability allows an unauthenticated attacker to reset Confluence and create a Confluence instance administrator account. Using this account, an attacker can then perform all administrative actions that are available to Confluence instance administrator leading to - but not limited to - full loss of confidentiality, integrity and availability. Atlassian Cloud sites are not affected by this vulnerability. If your Confluence site is accessed via an atlassian.net domain, it is hosted by Atlassian and is not vulnerable to this issue.	9.8	More Details
CVE-2023-5360	The Royal Elementor Addons and Templates WordPress plugin before 1.3.79 does not properly validate uploaded files, which could allow unauthenticated users to upload arbitrary files, such as PHP and achieve RCE.	9.8	More Details
CVE-2023-46979	TOTOLINK X6000R V9.4.0cu.852_B20230719 was discovered to contain a command injection vulnerability via the enable parameter in the setLedCfg function.	9.8	More Details
CVE-2023-46977	TOTOLINK LR1200GB V9.1.0u.6619_B20230130 was discovered to contain a stack overflow via the password parameter in the function loginAuth.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46976	TOTOLINK A3300R 17.0.0cu.557_B20221024 contains a command injection via the file_name parameter in the UploadFirmwareFile function.	9.8	More Details
CVE-2023-43139	An issue in franfinance before v.2.0.27 allows a remote attacker to execute arbitrary code via the validation.php, and controllers/front/validation.php components.	9.8	More Details
CVE-2023-46510	An issue in ZIONCOM (Hong Kong) Technology Limited A7000R v.4.1cu.4154 allows an attacker to execute arbitrary code via the cig-bin/cstecgi.cgi to the settings/setPasswordCfg function.	9.8	More Details
CVE-2023-36263	Prestashop opartlimitquantity 1.4.5 and before is vulnerable to SQL Injection. OpartlimitquantityAlertlimitModuleFrontController::displayAjaxPushAlertMessage()` has sensitive SQL calls that can be executed with a trivial http call and exploited to forge a SQL injection.	9.8	More Details
CVE-2023-47174	Thorn SFTP gateway 3.4.x before 3.4.4 uses Pivotal Spring Framework for Java deserialization of untrusted data, which is not supported by Pivotal, a related issue to CVE-2016-1000027. Also, within the specific context of Thorn SFTP gateway, this leads to remote code execution.	9.8	More Details
CVE-2023-46356	In the module "CSV Feeds PRO" (csvfeeds) before 2.6.1 from Bl Modules for PrestaShop, a guest can perform SQL injection. The method `SearchApiCsv::getProducts()` has sensitive SQL call that can be executed with a trivial http call and exploited to forge a SQL injection.	9.8	More Details
CVE-2023-45378	In the module "PrestaBlog" (prestablog) version 4.4.7 and before from HDclic for PrestaShop, a guest can perform SQL injection. The script ajax slider_positions.php has a sensitive SQL call that can be executed with a trivial http call and exploited to forge a SQL injection.	9.8	More Details
CVE-2023-27846	SQL injection vulnerability found in PrestaShop themevolty v.4.0.8 and before allow a remote attacker to gain privileges via the tvcmsblog, tvcmsvideotab, tvcmswishlist, tvcmsbrandlist, tvcmscategorychainslider, tvcmscategoryproduct, tvcmscategoryslider, tvcmspaymenticon, tvcmstestimonial components.	9.8	More Details
CVE-2023-5865	Insufficient Session Expiration in GitHub repository thorsten/phpmyfaq prior to 3.2.2.	9.8	More Details
CVE-2023-46502	An issue in openCRX v.5.2.2 allows a remote attacker to read internal files and execute server side request forgery attack via insecure DocumentBuilderFactory.	9.8	More Details
CVE-2023-43792	baserCMS is a website development framework. In versions 4.6.0 through 4.7.6, there is a Code Injection vulnerability in the mail form of baserCMS. As of time of publication, no known patched versions are available.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-47104	tinyfiledialogs (aka tiny file dialogs) before 3.15.0 allows shell metacharacters (such as a backquote or a dollar sign) in titles, messages, and other input data. NOTE: this issue exists because of an incomplete fix for CVE-2020-36767, which only considered single and double quote characters.	9.8	More Details
CVE-2023-45797	A Buffer overflow vulnerability in DreamSecurity MagicLine4NX versions 1.0.0.1 to 1.0.0.26 allows an attacker to remotely execute code.	9.8	More Details
CVE-2021-33635	When malicious images are pulled by isula pull, attackers can execute arbitrary code.	9.8	More Details
CVE-2023-5838	Insufficient Session Expiration in GitHub repository linkstackorg/linkstack prior to v4.2.9.	9.8	More Details
CVE-2023-46570	An out-of-bounds read in radare2 v.5.8.9 and before exists in the print_insn32 function of libr/arch/p/nds32/nds32-dis.h.	9.8	More Details
CVE-2023-46410	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a command execution vulnerability via the sub_ The 416F60 function.	9.8	More Details
CVE-2023-46411	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a command execution vulnerability via the sub_415258 function.	9.8	More Details
CVE-2023-46413	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a command execution vulnerability via the sub_4155DC function.	9.8	More Details
CVE-2023-46409	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a command execution vulnerability via the sub_ 41CC04 function.	9.8	More Details
CVE-2023-46370	Tenda W18E V16.01.0.8(1576) has a command injection vulnerability via the hostName parameter in the formSetNetCheckTools function.	9.8	More Details
CVE-2023-46373	TP-Link TL-WDR7660 2.0.30 has a stack overflow vulnerability via the function deviceInfoJsonToBincauses.	9.8	More Details
CVE-2023-46518	Mercury A15 V1.0 20230818_1.0.3 was discovered to contain a command execution vulnerability via the component cloudDeviceTokenSuccCB.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46520	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function uninstallPluginReqHandle.	9.8	More Details
CVE-2023-46521	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function RegisterRegister.	9.8	More Details
CVE-2023-46522	TP-LINK device TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin and TL-WDR7660 2.0.30 were discovered to contain a stack overflow via the function deviceInfoRegister.	9.8	More Details
CVE-2023-46523	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function upgradeInfoRegister.	9.8	More Details
CVE-2023-46525	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function loginRegister.	9.8	More Details
CVE-2023-46526	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function resetCloudPwdRegister.	9.8	More Details
CVE-2023-46527	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin and TL-WDR7660 2.0.30 was discovered to contain a stack overflow via the function bindRequestHandle.	9.8	More Details
CVE-2023-46534	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function modifyAccPwdRegister.	9.8	More Details
CVE-2023-46535	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function getResetVeriRegister.	9.8	More Details
CVE-2023-46536	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function chkRegVeriRegister.	9.8	More Details
CVE-2023-46537	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function getRegVeriRegister.	9.8	More Details
CVE-2023-46538	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function chkResetVeriRegister.	9.8	More Details
CVE-2023-46408	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a command execution vulnerability via the sub_ The 41DD80 function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46371	TP-Link device TL-WDR7660 2.0.30 and TL-WR886N 2.0.12 has a stack overflow vulnerability via the function upgradeInfoJsonToBin.	9.8	More Details
CVE-2023-46369	Tenda W18E V16.01.0.8(1576) contains a stack overflow vulnerability via the portMirrorMirroredPorts parameter in the formSetNetCheckTools function.	9.8	More Details
CVE-2023-46541	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formIpv6Setup.	9.8	More Details
CVE-2023-46358	In the module "Referral and Affiliation Program" (referralbyphone) version 3.5.1 and before from Snegurka for PrestaShop, a guest can perform SQL injection. Method `ReferralByPhoneDefaultModuleFrontController::ajaxProcessCartRuleValidate` has sensitive SQL calls that can be executed with a trivial http call and exploited to forge a SQL injection.	9.8	More Details
CVE-2023-26572	Unauthenticated SQL injection in the GetExcursionList method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers.	9.8	More Details
CVE-2023-26581	Unauthenticated SQL injection in the GetVisitors method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers.	9.8	More Details
CVE-2023-26582	Unauthenticated SQL injection in the GetExcursionDetails method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers.	9.8	More Details
CVE-2023-26583	Unauthenticated SQL injection in the GetCurrentPeriod method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers.	9.8	More Details
CVE-2023-26584	Unauthenticated SQL injection in the GetStudentInconsistencies method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers.	9.8	More Details
CVE-2023-27254	Unauthenticated SQL injection in the GetRoomChanges method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers.	9.8	More Details
CVE-2023-27255	Unauthenticated SQL injection in the DeleteRoomChanges method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers.	9.8	More Details
CVE-2023-27260	Unauthenticated SQL injection in the GetAssignmentsDue method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27262	Unauthenticated SQL injection in the GetAssignmentsDue method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers.	9.8	More Details
CVE-2023-31581	Dromara Sureness before v1.0.8 was discovered to use a hardcoded key.	9.8	More Details
CVE-2023-34048	vCenter Server contains an out-of-bounds write vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger an out-of-bounds write potentially leading to remote code execution.	9.8	More Details
CVE-2023-44794	An issue in Dromara SaToken version 1.36.0 and before allows a remote attacker to escalate privileges via a crafted payload to the URL.	9.8	More Details
CVE-2023-45554	File Upload vulnerability in zzzCMS v.2.1.9 allows a remote attacker to execute arbitrary code via modification of the imageext parameter from jpg, jpeg,gif, and png to jpg, jpeg,gif, png, pphphp.	9.8	More Details
CVE-2023-46010	An issue in SeaCMS v.12.9 allows an attacker to execute arbitrary commands via the admin_safe.php component.	9.8	More Details
CVE-2023-46347	In the module "Step by Step products Pack" (ndk_steppingpack) version 1.5.6 and before from NDK Design for PrestaShop, a guest can perform SQL injection. The method `NdkSpack::getPacks()` has sensitive SQL calls that can be executed with a trivial http call and exploited to forge a SQL injection.	9.8	More Details
CVE-2023-46540	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formNtp.	9.8	More Details
CVE-2023-46539	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function registerRequestHandle.	9.8	More Details
CVE-2023-46557	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formMultiAPVLAN.	9.8	More Details
CVE-2023-46554	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formMapDel.	9.8	More Details
CVE-2023-5746	A vulnerability regarding use of externally-controlled format string is found in the cgi component. This allows remote attackers to execute arbitrary code via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.5-0185 may be affected: BC500 and TC500.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5731	Memory safety bugs present in Firefox 118. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 119.	9.8	More Details
CVE-2023-5730	Memory safety bugs present in Firefox 118, Firefox ESR 115.3, and Thunderbird 115.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	9.8	More Details
CVE-2023-46574	An issue in TOTOLINK A3700R v.9.1.2u.6165_20211012 allows a remote attacker to execute arbitrary code via the FileName parameter of the UploadFirmwareFile function.	9.8	More Details
CVE-2023-46564	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formDMZ.	9.8	More Details
CVE-2023-46563	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formIpQoS.	9.8	More Details
CVE-2023-46562	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formDosCfg.	9.8	More Details
CVE-2023-46560	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formTcpipSetup.	9.8	More Details
CVE-2023-46559	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formIPv6Addr.	9.8	More Details
CVE-2023-46558	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formMapDelDevice.	9.8	More Details
CVE-2023-46542	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formMeshUploadConfig.	9.8	More Details
CVE-2023-46556	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formFilter.	9.8	More Details
CVE-2023-46555	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formPortFw.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46485	An issue in TOTOlink X6000R V9.4.0cu.852_B20230719 allows a remote attacker to execute arbitrary code via the setTracerouteCfg function of the stecgi.cgi component.	9.8	More Details
CVE-2023-46553	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formParentControl.	9.8	More Details
CVE-2023-46550	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formMapDelDevice.	9.8	More Details
CVE-2023-46543	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formWlSiteSurvey.	9.8	More Details
CVE-2023-46544	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formWirelessTbl.	9.8	More Details
CVE-2023-46545	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formWsc.	9.8	More Details
CVE-2023-46546	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formStats.	9.8	More Details
CVE-2023-46547	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formSysLog.	9.8	More Details
CVE-2023-46548	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formWlanRedirect.	9.8	More Details
CVE-2023-46552	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formMultiAP.	9.8	More Details
CVE-2023-46549	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formSetLg.	9.8	More Details
CVE-2023-46551	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formReflashClientTbl.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46249	authentik is an open-source Identity Provider. Prior to versions 2023.8.4 and 2023.10.2, when the default admin user has been deleted, it is potentially possible for an attacker to set the password of the default admin user without any authentication. authentik uses a blueprint to create the default admin user, which can also optionally set the default admin users' password from an environment variable. When the user is deleted, the `initial-setup` flow used to configure authentik after the first installation becomes available again. authentik 2023.8.4 and 2023.10.2 fix this issue. As a workaround, ensure the default admin user (Username `akadmin`) exists and has a password set. It is recommended to use a very strong password for this user, and store it in a secure location like a password manager. It is also possible to deactivate the user to prevent any logins as akadmin.	9.6	More Details
CVE-2023-45136	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. When document names are validated according to a name strategy (disabled by default), XWiki starting in version 12.0-rc-1 and prior to versions 12.10.12 and 15.5-rc-1 is vulnerable to a reflected cross-site scripting attack in the page creation form. This allows an attacker to execute arbitrary actions with the rights of the user opening the malicious link. Depending on the rights of the user, this may allow remote code execution and full read and write access to the whole XWiki installation. This has been patched in XWiki 14.10.12 and 15.5-rc-1 by adding appropriate escaping. The vulnerable template file `createinline.vm` is part of XWiki's WAR and can be patched by manually applying the changes from the fix.	9.6	More Details
CVE-2023-5820	The Thumbnail Slider With Lightbox plugin for WordPress is vulnerable to Cross-Site Request Forgery in version 1.0. This is due to missing or incorrect nonce validation on the addedit functionality. This makes it possible for unauthenticated attackers to upload arbitrary files via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	9.6	More Details
CVE-2023-5832	Improper Input Validation in GitHub repository mintplex-labs/anything-llm prior to 0.1.0.	9.1	More Details
CVE-2023-5754	Sielco PolyEco1000 uses a weak set of default administrative credentials that can be easily guessed in remote password attacks and gain full control of the system.	9.1	More Details
CVE-2023-46133	CryptoES is a cryptography algorithms library compatible with ES6 and TypeScript. Prior to version 2.1.0, CryptoES PBKDF2 is 1,000 times weaker than originally specified in 1993, and at least 1,300,000 times weaker than current industry standard. This is because it both defaults to SHA1, a cryptographic hash algorithm considered insecure since at least 2005, and defaults to one single iteration, a 'strength' or 'difficulty' value specified at 1,000 when specified in 1993. PBKDF2 relies on iteration count as a countermeasure to preimage and collision attacks. If used to protect passwords, the impact is high. If used to generate signatures, the impact is high. Version 2.1.0 contains a patch for this issue. As a workaround, configure CryptoES to use SHA256 with at least 250,000 iterations.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46233	crypto-js is a JavaScript library of crypto standards. Prior to version 4.2.0, crypto-js PBKDF2 is 1,000 times weaker than originally specified in 1993, and at least 1,300,000 times weaker than current industry standard. This is because it both defaults to SHA1, a cryptographic hash algorithm considered insecure since at least 2005, and defaults to one single iteration, a 'strength' or 'difficulty' value specified at 1,000 when specified in 1993. PBKDF2 relies on iteration count as a countermeasure to preimage and collision attacks. If used to protect passwords, the impact is high. If used to generate signatures, the impact is high. Version 4.2.0 contains a patch for this issue. As a workaround, configure crypto-js to use SHA256 with at least 250,000 iterations.	9.1	More Details
CVE-2023-37908	XWiki Rendering is a generic Rendering system that converts textual input in a given syntax into another syntax. The cleaning of attributes during XHTML rendering, introduced in version 14.6-rc-1, allowed the injection of arbitrary HTML code and thus cross-site scripting via invalid attribute names. This can be exploited, e.g., via the link syntax in any content that supports XWiki syntax like comments in XWiki. When a user moves the mouse over a malicious link, the malicious JavaScript code is executed in the context of the user session. When this user is a privileged user who has programming rights, this allows server-side code execution with programming rights, impacting the confidentiality, integrity and availability of the XWiki instance. While this attribute was correctly recognized as not allowed, the attribute was still printed with a prefix `data-xwiki-translated-attribute-` without further cleaning or validation. This problem has been patched in XWiki 14.10.4 and 15.0 RC1 by removing characters not allowed in data attributes and then validating the cleaned attribute again. There are no known workarounds apart from upgrading to a version including the fix.	9.0	More Details
CVE-2023-45137	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. `org.xwiki.platform:xwiki-platform-web` starting in version 3.1-milestone-2 and prior to version 13.4-rc-1, as well as `org.xwiki.platform:xwiki-platform-web-templates` prior to versions 14.10.12 and 15.5-rc-1, are vulnerable to cross-site scripting. When trying to create a document that already exists, XWiki displays an error message in the form for creating it. Due to missing escaping, this error message is vulnerable to raw HTML injection and thus XSS. The injected code is the document reference of the existing document so this requires that the attacker first creates a non-empty document whose name contains the attack code. This has been patched in `org.xwiki.platform:xwiki-platform-web` version 13.4-rc-1 and `org.xwiki.platform:xwiki-platform-web-templates` versions 14.10.12 and 15.5-rc-1 by adding the appropriate escaping. The vulnerable template file `createinline.vm` is part of XWiki's WAR and can be patched by manually applying the changes from the fix.	9.0	More Details
CVE-2023-5843	The Ads by datafeedr.com plugin for WordPress is vulnerable to Remote Code Execution in versions up to, and including, 1.1.3 via the 'dfads_ajax_load_ads' function. This allows unauthenticated attackers to execute code on the server. The parameters of the callable function are limited, they cannot be specified arbitrarily.	9.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31422	An issue was discovered by Elastic whereby sensitive information is recorded in Kibana logs in the event of an error. The issue impacts only Kibana version 8.10.0 when logging in the JSON layout or when the pattern layout is configured to log the %meta pattern. Elastic has released Kibana 8.10.1 which resolves this issue. The error object recorded in the log contains request information, which can include sensitive data, such as authentication credentials, cookies, authorization headers, query params, request paths, and other metadata. Some examples of sensitive data which can be included in the logs are account credentials for kibana_system, kibana-metricbeat, or Kibana end-users.	9.0	More Details
CVE-2023-45869	ILIAS 7.25 (2023-09-12) allows any authenticated user to execute arbitrary operating system commands remotely, when a highly privileged account accesses an XSS payload. The injected commands are executed via the exec() function in the execQuoted() method of the ilUtil class (/Services/Utilities/classes/class.ilUtil.php) This allows attackers to inject malicious commands into the system, potentially compromising the integrity, confidentiality, and availability of the ILIAS installation and the underlying operating system.	9.0	More Details
CVE-2023-45134	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. `org.xwiki.platform:xwiki-platform-web` starting in version 3.1-milestone-1 and prior to 13.4-rc-1, `org.xwiki.platform:xwiki-platform-web-templates` prior to versions 14.10.2 and 15.5-rc-1, and `org.xwiki.platform:xwiki-web-standard` starting in version 2.4-milestone-2 and prior to version 3.1-milestone-1 are vulnerable to cross-site scripting. An attacker can create a template provider on any document that is part of the wiki (could be the attacker's user profile) that contains malicious code. This code is executed when this template provider is selected during document creation which can be triggered by sending the user to a URL. For the attacker, the only requirement is to have an account as by default the own user profile is editable. This allows an attacker to execute arbitrary actions with the rights of the user opening the malicious link. Depending on the rights of the user, this may allow remote code execution and full read and write access to the whole XWiki installation. This has been patched in `org.xwiki.platform:xwiki-platform-web` 13.4-rc-1, `org.xwiki.platform:xwiki-platform-web-templates` 14.10.2 and 15.5-rc-1, and `org.xwiki.platform:xwiki-web-standard` 3.1-milestone-1 by adding the appropriate escaping. The vulnerable template file createinline.vm is part of XWiki's WAR and can be patched by manually applying the changes from the fix.	9.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45135	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In `org.xwiki.platform:xwiki-platform-web` versions 7.2-milestone-2 until 14.10.12 and `org.xwiki.platform:xwiki-platform-web-templates` prior to versions 14.10.12 and 15.5-rc-1, it is possible to pass a title to the page creation action that isn't displayed at first but then executed in the second step. This can be used by an attacker to trick a victim to execute code, allowing script execution if the victim has script right or remote code execution including full access to the XWiki instance if the victim has programming right. For the attack to work, the attacker needs to convince the victim to visit a link like `<xwiki-host>/xwiki/bin/create/NonExistingSpace/WebHome?title=$services.logging.getLogger(%22foo%22).error(%22Script%20executed!%22)` where `<xwiki-host>` is the URL of the Wiki installation and to then click on the "Create" button on that page. The page looks like a regular XWiki page that the victim would also see when clicking the button to create a page that doesn't exist yet, the malicious code is not displayed anywhere on that page. After clicking the "Create" button, the malicious title would be displayed but at this point, the code has already been executed and the attacker could use this code also to hide the attack, e.g., by redirecting the victim again to the same page with an innocent title. It thus seems plausible that this attack could work if the attacker can place a fake "create page" button on a page which is possible with edit right. This has been patched in `org.xwiki.platform:xwiki-platform-web` version 14.10.12 and `org.xwiki.platform:xwiki-platform-web-templates` versions 14.10.12 and 15.5-rc-1 by displaying the title already in the first step such that the victim can notice the attack before continuing. It is possible to manually patch the modified files from the patch in an existing installation. For the JavaScript change, the minified JavaScript file would need to be obtained from a build of XWiki and replaced accordingly.	9.0	More Details
CVE-2023-46248	Cody is an artificial intelligence (AI) coding assistant. The Cody AI VSCode extension versions 0.10.0 through 0.14.0 are vulnerable to Remote Code Execution under certain conditions. An attacker in control of a malicious repository could modify the Cody configuration file `.vscode/cody.json` and overwrite Cody commands. If a user with the extension installed opens this malicious repository and runs a Cody command such as /explain or /doc, this could allow arbitrary code execution on the user's machine. The vulnerability is rated as critical severity, but with low exploitability. It requires the user to have a malicious repository loaded and execute the overwritten command in VS Code. The issue is exploitable regardless of the user blocking code execution on a repository through VS Code Workspace Trust. The issue was found during a regular 3rd party penetration test. The maintainers of Cody do not have evidence of open source repositories having malicious `.vscode/cody.json` files to exploit this vulnerability. The issue is fixed in version 0.14.1 of the Cody VSCode extension. In case users can't promptly upgrade, they should not open any untrusted repositories with the Cody extension loaded.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-46723	lte-pic32-writer is a writer for PIC32 devices. In versions 0.0.1 and prior, those who use `sendto.txt` are vulnerable to attackers who known the IMEI reading the sendto.txt. The sendto.txt file can contain the SNS(such as slack and zulip) URL and API key. As of time of publication, a patch is not yet available. As workarounds, avoid using `sendto.txt` or use `.htaccess` to block access to `sendto.txt`.	8.9	More Details
CVE-2023-44480	Leave Management System Project v1.0 is vulnerable to multiple Authenticated SQL Injection vulnerabilities. The 'setcasualleave' parameter of the admin/setleaves.php resource does not validate the characters received and they are sent unfiltered to the database.	8.8	More Details
CVE-2022-34886	A remote code execution vulnerability was found in the firmware used in some Lenovo printers, which can be caused by a remote user pushing an illegal string to the server-side interface via a script, resulting in a stack overflow.	8.8	More Details
CVE-2023-5433	The Message ticker plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 9.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2023-42491	EisBaer Scada - CWE-285: Improper Authorization	8.8	More Details
CVE-2023-5431	The Left right image slideshow gallery plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 12.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2023-5840	Weak Password Recovery Mechanism for Forgotten Password in GitHub repository linkstackorg/linkstack prior to v4.2.9.	8.8	More Details
CVE-2023-40447	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution.	8.8	More Details
CVE-2023-41255	The vulnerability allows an unprivileged user with access to the subnet of the TPC-110W device to gain a root shell on the device itself abusing the lack of authentication of the ‘su’ binary file installed on the device that can be accessed through the ADB (Android Debug Bridge) protocol exposed on the network.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5430	The Jquery news ticker plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 3.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2023-42658	Archive command in Chef InSpec prior to 4.56.58 and 5.22.29 allow local command execution via maliciously crafted profile.	8.8	More Details
CVE-2023-41976	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution.	8.8	More Details
CVE-2023-5429	The Information Reel plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 10.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2023-5428	The Image vertical reel scroll slideshow plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 9.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2023-21392	In Bluetooth, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege when connecting to a Bluetooth device with no additional execution privileges needed. User interaction is not needed for exploitation.	8.8	More Details
CVE-2023-5412	The Image horizontal reel scroll slideshow plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 13.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2022-38484	An arbitrary file upload and directory traversal vulnerability exist in the file upload functionality of the System Setup menu in AgeVolt Portal prior to version 0.1. A remote authenticated attacker could leverage this vulnerability to upload files to any location on the target operating system with web server privileges.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5434	The Superb slideshow gallery plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 13.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2023-45851	The Android Client application, when enrolled to the AppHub server,connects to an MQTT broker without enforcing any server authentication. This issue allows an attacker to force the Android Client application to connect to a malicious MQTT broker, enabling it to send fake messages to the HMI device	8.8	More Details
CVE-2023-42852	A logic issue was addressed with improved checks. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution.	8.8	More Details
CVE-2023-5435	The Up down image slideshow gallery plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 12.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2023-5311	The WP EXtra plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the register() function in versions up to, and including, 6.2. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to modify the contents of the .htaccess files located in a site's root directory or /wp-content and /wp-includes folders and achieve remote code execution.	8.8	More Details
CVE-2023-5472	Use after free in Profiles in Google Chrome prior to 118.0.5993.117 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-5464	The Jquery accordion slideshow plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 8.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5439	The Wp photo text slider 50 plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 8.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2023-5833	Improper Access Control in GitHub repository mintplex-labs/anything-llm prior to 0.1.0.	8.8	More Details
CVE-2023-21361	In Bluetooth, there is a possibility of code-execution due to a use after free. This could lead to paired device escalation of privilege in the privileged Bluetooth process with no additional execution privileges needed. User interaction is not needed for exploitation.	8.8	More Details
CVE-2023-5438	The wp image slideshow plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 12.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2023-5315	The Google Maps made Simple plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 0.6 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2023-5437	The WP fade in text news plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 12.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2023-5583	The WP Simple Galleries plugin for WordPress is vulnerable to PHP Object Injection in versions up to, and including, 1.34 via deserialization of untrusted input from the 'wpsimplegallery_gallery' post meta via 'wpsgallery' shortcode. This allows authenticated attackers, with contributor-level permissions and above, to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5436	The Vertical marquee plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 7.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2023-45220	The Android Client application, when enrolled with the define method 1(the user manually inserts the server ip address), use HTTP protocol to retrieve sensitive information (ip address and credentials to connect to a remote MQTT broker entity) instead of HTTPS and this feature is not configurable by the user.	8.8	More Details
CVE-2023-43961	An issue in Dromara SaToken version 1.3.50RC and before when using Spring dynamic controllers, a specially crafted request may cause an authentication bypass.	8.8	More Details
CVE-2023-35794	An issue was discovered in Cassia Access Controller 2.1.1.2303271039. The Web SSH terminal endpoint (spawned console) can be accessed without authentication. Specifically, there is no session cookie validation on the Access Controller; instead, there is only Basic Authentication to the SSH console.	8.8	More Details
CVE-2023-21356	In Bluetooth, 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.	8.8	More Details
CVE-2023-46102	The Android Client application, when enrolled to the AppHub server, connects to an MQTT broker to exchange messages and receive commands to execute on the HMI device. The protocol builds on top of MQTT to implement the remote management of the device is encrypted with a hard-coded DES symmetric key, that can be retrieved reversing both the Android Client application and the server-side web application. This issue allows an attacker able to control a malicious MQTT broker on the same subnet network of the device, to craft malicious messages and send them to the HMI device, executing arbitrary commands on the device itself.	8.8	More Details
CVE-2023-40129	In build_read_multi_rsp of gatt_sr.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	8.8	More Details
CVE-2023-5798	The Assistant WordPress plugin before 1.4.4 does not validate a parameter before making a request to it via wp_remote_get(), which could allow users with a role as low as Editor to perform SSRF attacks	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5425	The Post Meta Data Manager plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the pmdm_wp_change_user_meta and pmdm_wp_change_post_meta functions in versions up to, and including, 1.2.0. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to gain elevated (e.g., administrator) privileges.	8.8	More Details
CVE-2023-3955	A security issue was discovered in Kubernetes where a user that can create pods on Windows nodes may be able to escalate to admin privileges on those nodes. Kubernetes clusters are only affected if they include Windows nodes.	8.8	More Details
CVE-2023-46449	Sourcecodester Free and Open Source inventory management system v1.0 is vulnerable to Incorrect Access Control. An arbitrary user can change the password of another user and takeover the account via IDOR in the password change function.	8.8	More Details
CVE-2023-46748	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	8.8	More Details
CVE-2023-46815	An issue was discovered in SugarCRM 12 before 12.0.4 and 13 before 13.0.2. An Unrestricted File Upload vulnerability has been identified in the Notes module. By using a crafted request, custom PHP code can be injected via the Notes module because of missing input validation. An attacker with regular user privileges can exploit this.	8.8	More Details
CVE-2023-20886	VMware Workspace ONE UEM console contains an open redirect vulnerability. A malicious actor may be able to redirect a victim to an attacker and retrieve their SAML response to login as the victim user.	8.8	More Details
CVE-2023-46816	An issue was discovered in SugarCRM 12 before 12.0.4 and 13 before 13.0.2. A Server Site Template Injection (SSTI) vulnerability has been identified in the GecControl action. By using a crafted request, custom PHP code can be injected via the GetControl action because of missing input validation. An attacker with regular user privileges can exploit this.	8.8	More Details
CVE-2023-28777	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LearnDash LearnDash LMS allows SQL Injection.This issue affects LearnDash LMS: from n/a through 4.5.3.	8.8	More Details
CVE-2022-4886	Ingress-nginx `path` sanitization can be bypassed with `log_format` directive.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5099	The HTML filter and csv-file search plugin for WordPress is vulnerable to Local File Inclusion in versions up to, and including, 2.7 via the 'src' attribute of the 'csvsearch' shortcode. This allows authenticated attackers, with contributor-level permissions and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other “safe” file types can be uploaded and included.	8.8	More Details
CVE-2023-45996	SQL injection vulnerability in Senayan Library Management Systems Slims v.9 and Bulian v.9.6.1 allows a remote attacker to obtain sensitive information and execute arbitrary code via a crafted script to the reborrowLimit parameter in the member_type.php.	8.8	More Details
CVE-2023-0897	Sielco PolyEco1000 is vulnerable to a session hijack vulnerability due to the cookie being vulnerable to a brute force attack, lack of SSL, and the session being visible in requests.	8.8	More Details
CVE-2023-46375	ZenTao Biz version 4.1.3 and before is vulnerable to Cross Site Request Forgery (CSRF).	8.8	More Details
CVE-2023-3676	A security issue was discovered in Kubernetes where a user that can create pods on Windows nodes may be able to escalate to admin privileges on those nodes. Kubernetes clusters are only affected if they include Windows nodes.	8.8	More Details
CVE-2023-33559	A local file inclusion vulnerability via the lang parameter in OcoMon before v4.0.1 allows attackers to execute arbitrary code by supplying a crafted PHP file.	8.8	More Details
CVE-2023-26578	Arbitrary file upload to web root in the IDAttend’s IDWeb application 3.1.013 allows authenticated attackers to upload dangerous files to web root such as ASP or ASPX, gaining command execution on the affected server.	8.8	More Details
CVE-2023-43322	ZPE Systems, Inc Nodegrid OS v5.0.0 to v5.0.17, v5.2.0 to v5.2.19, v5.4.0 to v5.4.16, v5.6.0 to v5.6.13, v5.8.0 to v5.8.10, and v5.10.0 to v5.10.3 was discovered to contain a command injection vulnerability via the endpoint /v1/system/toolkit/files/.	8.8	More Details
CVE-2023-42323	Cross Site Request Forgery (CSRF) vulnerability in DouHaocms v.3.3 allows a remote attacker to execute arbitrary code via the adminAction.class.php file.	8.8	More Details
CVE-2018-16739	An issue was discovered on certain ABUS TVIP devices. Due to a path traversal in /opt/cgi/admin/filewrite, an attacker can write to files, and thus execute code arbitrarily with root privileges.	8.8	More Details
CVE-2023-34446	iTop is an open source, web-based IT service management platform. Prior to versions 3.0.4 and 3.1.0, when displaying `pages/preferences.php`, cross site scripting is possible. This issue is fixed in versions 3.0.4 and 3.1.0.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45317	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site.	8.8	More Details
CVE-2023-34447	iTop is an open source, web-based IT service management platform. Prior to versions 3.0.4 and 3.1.0, on `pages/UI.php`, cross site scripting is possible. This issue is fixed in versions 3.0.4 and 3.1.0.	8.8	More Details
CVE-2023-46478	An issue in minCal v.1.0.0 allows a remote attacker to execute arbitrary code via a crafted script to the customer_data parameter.	8.8	More Details
CVE-2023-46238	ZITADEL is an identity infrastructure management system. ZITADEL users can upload their own avatar image using various image types including SVG. SVG can include scripts, such as javascript, which can be executed during rendering. Due to a missing security header, an attacker could inject code to an SVG to gain access to the victim's account in certain scenarios. A victim would need to directly open the malicious image in the browser, where a single session in ZITADEL needs to be active for this exploit to work. If the possible victim had multiple or no active sessions in ZITADEL, the attack would not succeed. This issue has been patched in version 2.39.2 and 2.38.2.	8.7	More Details
CVE-2023-43795	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. The OGC Web Processing Service (WPS) specification is designed to process information from any server using GET and POST requests. This presents the opportunity for Server Side Request Forgery. This vulnerability has been patched in version 2.22.5 and 2.23.2.	8.6	More Details
CVE-2023-46236	FOG is a free open-source cloning/imaging/rescue suite/inventory management system. Prior to version 1.5.10, a server-side-request-forgery (SSRF) vulnerability allowed an unauthenticated user to trigger a GET request as the server to an arbitrary endpoint and URL scheme. This also allows remote access to files visible to the Apache user group. Other impacts vary based on server configuration. Version 1.5.10 contains a patch.	8.6	More Details
CVE-2023-41339	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. The WMS specification defines an ``sld=<url>`` parameter for GetMap, GetLegendGraphic and GetFeatureInfo operations for user supplied "dynamic styling". Enabling the use of dynamic styles, without also configuring URL checks, provides the opportunity for Service Side Request Forgery. This vulnerability can be used to steal user NetNTLMv2 hashes which could be relayed or cracked externally to gain further access. This vulnerability has been patched in versions 2.22.5 and 2.23.2.	8.6	More Details
CVE-2023-45798	In Yettiesoft VestCert versions 2.36 to 2.5.29, a vulnerability exists due to improper validation of third-party modules. This allows malicious actors to load arbitrary third-party modules, leading to remote code execution.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33638	When the isula cp command is used to copy files from a container to a host machine and the container is controlled by an attacker, the attacker can escape the container.	8.4	More Details
CVE-2021-33637	When the isula export command is used to export a container to an image and the container is controlled by an attacker, the attacker can escape the container.	8.4	More Details
CVE-2021-33636	When the isula load command is used to load malicious images, attackers can execute arbitrary code.	8.4	More Details
CVE-2023-45321	The Android Client application, when enrolled with the define method 1 (the user manually inserts the server ip address), use HTTP protocol to retrieve sensitive information (ip address and credentials to connect to a remote MQTT broker entity) instead of HTTPS and this feature is not configurable by the user. Due to the lack of encryption of HTTP,this issue allows an attacker placed in the same subnet network of the HMI device to intercept username and password necessary to authenticate to the MQTT server responsible to implement the remote management protocol.	8.3	More Details
CVE-2023-46124	Fides is an open-source privacy engineering platform for managing the fulfillment of data privacy requests in runtime environments, and the enforcement of privacy regulations in code. The Fides web application allows a custom integration to be uploaded as a ZIP file containing configuration and dataset definitions in YAML format. It was discovered that specially crafted YAML dataset and config files allow a malicious user to perform arbitrary requests to internal systems and exfiltrate data outside the environment (also known as a Server-Side Request Forgery). The application does not perform proper validation to block attempts to connect to internal (including localhost) resources. The vulnerability has been patched in Fides version `2.22.1`.	8.2	More Details
CVE-2023-39732	The leakage of the client secret in Tokueimaru_waiting Line 13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages.	8.2	More Details
CVE-2023-39733	The leakage of the client secret in TonTon-Tei Line v13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages.	8.2	More Details
CVE-2023-39734	The leakage of the client secret in VISION MEAT WORKS TrackDiner10/10_mc Line v13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages.	8.2	More Details
CVE-2023-39735	The leakage of the client secret in Uomasa_Saiji_news Line 13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39736	The leakage of the client secret in Fukunaga_memberscard Line 13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages.	8.2	More Details
CVE-2023-39737	The leakage of the client secret in Matsuya Line 13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages.	8.2	More Details
CVE-2023-26573	Missing authentication in the SetDB method in IDAttend's IDWeb application 3.1.052 and earlier allows denial of service or theft of database login credentials.	8.2	More Details
CVE-2023-39739	The leakage of the client secret in REGINA SWEETS&BAKERY Line 13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages.	8.2	More Details
CVE-2023-4967	Denial of Service in NetScaler ADC and NetScaler Gateway when configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA Virtual Server	8.2	More Details
CVE-2023-39740	The leakage of the client secret in Onigiriya-musubee Line 13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages.	8.2	More Details
CVE-2023-30969	The Palantir Tiles1 service was found to be vulnerable to an API wide issue where the service was not performing authentication/authorization on all the endpoints.	8.2	More Details
CVE-2023-4964	Potential open redirect vulnerability in opentext Service Management Automation X (SMAX) versions 2020.05, 2020.08, 2020.11, 2021.02, 2021.05, 2021.08, 2021.11, 2022.05, 2022.11 and opentext Asset Management X (AMX) versions 2021.08, 2021.11, 2022.05, 2022.11. The vulnerability could allow attackers to redirect a user to malicious websites.	8.2	More Details
CVE-2023-45868	The Learning Module in ILIAS 7.25 (2023-09-12 release) allows an attacker (with basic user privileges) to achieve a high-impact Directory Traversal attack on confidentiality and availability. By exploiting this network-based vulnerability, the attacker can move specified directories, normally outside the documentRoot, to a publicly accessible location via the PHP function rename(). This results in a total loss of confidentiality, exposing sensitive resources, and potentially denying access to the affected component and the operating system's components. To exploit this, an attacker must manipulate a POST request during the creation of an exercise unit, by modifying the old_name and new_name parameters via directory traversal. However, it's essential to note that, when exploiting this vulnerability, the specified directory will be relocated from its original location, rendering all files obtained from there unavailable.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37910	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Starting with the introduction of attachment move support in version 14.0-rc-1 and prior to versions 14.4.8, 14.10.4, and 15.0-rc-1, an attacker with edit access on any document (can be the user profile which is editable by default) can move any attachment of any other document to this attacker-controlled document. This allows the attacker to access and possibly publish any attachment of which the name is known, regardless if the attacker has view or edit rights on the source document of this attachment. Further, the attachment is deleted from the source document. This vulnerability has been patched in XWiki 14.4.8, 14.10.4, and 15.0 RC1. There is no workaround apart from upgrading to a fixed version.	8.1	More Details
CVE-2023-4606	An authenticated XCC user with Read-Only permission can change a different user’s password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected.	8.1	More Details
CVE-2023-5098	The Campaign Monitor Forms by Optin Cat WordPress plugin before 2.5.6 does not prevent users with low privileges (like subscribers) from overwriting any options on a site with the string "true", which could lead to a variety of outcomes, including DoS.	8.1	More Details
CVE-2016-1203	Improper file verification vulnerability in SaAT Netizen installer ver.1.2.0.424 and earlier, and SaAT Netizen ver.1.2.0.8 (Build427) and earlier allows a remote unauthenticated attacker to conduct a man-in-the-middle attack. A successful exploitation may result in a malicious file being downloaded and executed.	8.1	More Details
CVE-2022-3007	The vulnerability exists in Syska SW100 Smartwatch due to an improper implementation and/or configuration of Nordic Device Firmware Update (DFU) which is used for performing Over-The-Air (OTA) firmware updates on the Bluetooth Low Energy (BLE) devices. An unauthenticated attacker could exploit this vulnerability by setting arbitrary values to handle on the vulnerable device over Bluetooth. Successful exploitation of this vulnerability could allow the attacker to perform firmware update, device reboot or data manipulation on the target device.	8.1	More Details
CVE-2023-46667	An issue was discovered in Fleet Server >= v8.10.0 and < v8.10.3 where Agent enrolment tokens are being inserted into the Fleet Server’s log file in plain text. These enrolment tokens could allow someone to enrol an agent into an agent policy, and potentially use that to retrieve other secrets in the policy including for Elasticsearch and third-party services. Alternatively a threat actor could potentially enrol agents to the clusters and send arbitrary events to Elasticsearch.	8.1	More Details
CVE-2023-46654	Jenkins CloudBees CD Plugin 1.1.32 and earlier follows symbolic links to locations outside of the expected directory during the cleanup process of the 'CloudBees CD - Publish Artifact' post-build step, allowing attackers able to configure jobs to delete arbitrary files on the Jenkins controller file system.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46290	Due to inadequate code logic, a previously unauthenticated threat actor could potentially obtain a local Windows OS user token through the FactoryTalk® Services Platform web service and then use the token to log in into FactoryTalk® Services Platform . This vulnerability can only be exploited if the authorized user did not previously log in into the FactoryTalk® Services Platform web service.	8.1	More Details
CVE-2023-37283	Under a very specific and highly unrecommended configuration, authentication bypass is possible in the PingFederate Identifier First Adapter	8.1	More Details
CVE-2023-45990	Insecure Permissions vulnerability in WenwenaiCMS v.1.0 allows a remote attacker to escalate privileges.	8.0	More Details
CVE-2023-46136	Werkzeug is a comprehensive WSGI web application library. If an upload of a file that starts with CR or LF and then is followed by megabytes of data without these characters: all of these bytes are appended chunk by chunk into internal bytearray and lookup for boundary is performed on growing buffer. This allows an attacker to cause a denial of service by sending crafted multipart data to an endpoint that will parse it. The amount of CPU time required can block worker processes from handling legitimate requests. This vulnerability has been patched in version 3.0.1.	8.0	More Details
CVE-2023-43488	The vulnerability allows a low privileged (untrusted) application to modify a critical system property that should be denied, in order to enable the ADB (Android Debug Bridge) protocol to be exposed on the network, exploiting it to gain a privileged shell on the device without requiring the physical access through USB.	7.9	More Details
CVE-2023-38994	The 'check_univention_joinstatus' prometheus monitoring script (and other scripts) in UCS 5.0-5 revealed the LDAP plaintext password of the machine account in the process list allowing attackers with local ssh access to gain higher privileges and perform followup attacks. By default, the configuration of UCS does not allow local ssh access for regular users.	7.9	More Details
CVE-2023-46587	Buffer Overflow vulnerability in XnView Classic v.2.51.5 allows a local attacker to execute arbitrary code via a crafted TIF file.	7.8	More Details
CVE-2023-40130	In onBindingDied of CallRedirectionProcessor.java, there is a possible permission bypass due to a logic error in the code. This could lead to local escalation of privilege and background activity launch with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-21378	In Telecomm, there is a possible way to silence the ring for calls of secondary users 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.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21381	In Media Resource Manager, there is a possible local arbitrary code execution due to use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-40128	In several functions of xmlregexp.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.	7.8	More Details
CVE-2023-40140	In android_view_InputDevice_create of android_view_InputDevice.cpp, there is a possible way to execute arbitrary code due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-40423	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-40125	In onCreate of ApnEditor.java, there is a possible way for a Guest user to change the APN due to a permission bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-42841	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-39427	In Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, and Cobalt Share v12 SP0 Build (1204.77), the affected applications lack proper validation of user-supplied data when parsing XE files. This could lead to an out-of-bounds write. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2023-39936	In Ashlar-Vellum Graphite v13.0.48, the affected application lacks proper validation of user-supplied data when parsing VC6 files. This could lead to an out-of-bounds read. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2023-43352	An issue in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted payload to the Content Manager Menu component.	7.8	More Details
CVE-2023-47101	The installer (aka openvpn-client-installer) in Securepoint SSL VPN Client before 2.0.40 allows local privilege escalation during installation or repair.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21398	In sdksandbox, there is a possible strandhogg style overlay attack 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.	7.8	More Details
CVE-2023-21397	In Setup Wizard, there is a possible way to save a WiFi network due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-21396	In Activity Manager, there is a possible background activity launch due to a logic error in the code. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-5367	A out-of-bounds write flaw was found in the xorg-x11-server. This issue occurs due to an incorrect calculation of a buffer offset when copying data stored in the heap in the XIChangeDeviceProperty function in Xi/xiproperty.c and in RRChangeOutputProperty function in randr/rrproperty.c, allowing for possible escalation of privileges or denial of service.	7.8	More Details
CVE-2023-34057	VMware Tools contains a local privilege escalation vulnerability. A malicious actor with local user access to a guest virtual machine may elevate privileges within the virtual machine.	7.8	More Details
CVE-2023-42856	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. Processing a file may lead to unexpected app termination or arbitrary code execution.	7.8	More Details
CVE-2023-44219	A local privilege escalation vulnerability in SonicWall Directory Services Connector Windows MSI client 4.1.21 and earlier versions allows a local low-privileged user to gain system privileges through running the recovery feature.	7.8	More Details
CVE-2023-21393	In Settings, there is a possible way for the user to change SIM 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.	7.8	More Details
CVE-2023-40120	In multiple locations, there is a possible way to bypass user notification of foreground services 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.	7.8	More Details
CVE-2023-27854	An arbitrary code execution vulnerability was reported to Rockwell Automation in Arena Simulation that could potentially allow a malicious user to commit unauthorized arbitrary code to the software by using a memory buffer overflow. The threat-actor could then execute malicious code on the system affecting the confidentiality, integrity, and availability of the product. The user would need to open a malicious file provided to them by the attacker for the code to execute.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27858	Rockwell Automation Arena Simulation contains an arbitrary code execution vulnerability that could potentially allow a malicious user to commit unauthorized code to the software by using an uninitialized pointer in the application. The threat-actor could then execute malicious code on the system affecting the confidentiality, integrity, and availability of the product. The user would need to open a malicious file provided to them by the attacker for the code to execute.	7.8	More Details
CVE-2023-21390	In Sim, there is a possible way to evade mobile preference restrictions due to a permission bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-40404	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Sonoma 14.1. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-3701	A privilege elevation vulnerability was reported in the Lenovo Vantage SystemUpdate plugin version 2.0.0.212 and earlier that could allow a local attacker to execute arbitrary code with elevated privileges.	7.8	More Details
CVE-2023-21389	In Settings, there is a possible bypass of profile owner restrictions 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.	7.8	More Details
CVE-2023-21388	In Settings, there is a possible restriction bypass 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.	7.8	More Details
CVE-2023-5717	A heap out-of-bounds write vulnerability in the Linux kernel's Linux Kernel Performance Events (perf) component can be exploited to achieve local privilege escalation. If perf_read_group() is called while an event's sibling_list is smaller than its child's sibling_list, it can increment or write to memory locations outside of the allocated buffer. We recommend upgrading past commit 32671e3799ca2e4590773fd0e63aaa4229e50c06.	7.8	More Details
CVE-2023-5671	HP Print and Scan Doctor for Windows may potentially be vulnerable to escalation of privilege. HP is releasing software updates to mitigate the potential vulnerability.	7.8	More Details
CVE-2023-40116	In onTaskAppeared of PipTaskOrganizer.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.	7.8	More Details
CVE-2023-40117	In resetSettingsLocked of SettingsProvider.java, there is a possible lockscreen bypass due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46468	An issue in juzawebCMS v.3.4 and before allows a remote attacker to execute arbitrary code via a crafted file to the custom plugin function.	7.8	More Details
CVE-2023-21351	In multiple locations, there is a possible background activity launch 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.	7.8	More Details
CVE-2023-21342	In Speech, there is a possible way to bypass background activity launch 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.	7.8	More Details
CVE-2023-21341	In Permission Manager, there is a possible way to bypass required permissions 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.	7.8	More Details
CVE-2023-21358	In UWB Google, there is a possible way for a malicious app to masquerade as system app com.android.uwb.resources due to improperly used crypto. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-21324	In Package Installer, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-44141	Inkdrop prior to v5.6.0 allows a local attacker to conduct a code injection attack by having a legitimate user open a specially crafted markdown file.	7.8	More Details
CVE-2023-45555	File Upload vulnerability in zzzCMS v.2.1.9 allows a remote attacker to execute arbitrary code via a crafted file to the down_url function in zzz.php file.	7.8	More Details
CVE-2021-39810	In NFC, there is a possible way to setup a default contactless payment app without user consent due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-21328	In Package Installer, there is a possible way to determine whether an app is installed, without query permissions, 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.	7.8	More Details
CVE-2023-21337	In InputMethod, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21298	In Slice, there is a possible disclosure of installed applications due to side channel information disclosure. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-21343	In ActivityStarter, there is a possible background activity launch due to an unsafe PendingIntent. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-21313	In Core, there is a possible way to forward calls without user knowledge 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.	7.8	More Details
CVE-2023-43506	A vulnerability in the ClearPass OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges to those of a higher role. A successful exploit allows malicious users to execute arbitrary code with root level privileges on the Linux instance.	7.8	More Details
CVE-2022-3699	A privilege escalation vulnerability was reported in the Lenovo HardwareScanPlugin prior to version 1.3.1.2 and Lenovo Diagnostics prior to version 4.45 that could allow a local user to execute code with elevated privileges.	7.8	More Details
CVE-2023-5839	Privilege Chaining in GitHub repository hestiacp/hestiacp prior to 1.8.9.	7.8	More Details
CVE-2023-5739	Certain versions of HP PC Hardware Diagnostics Windows are potentially vulnerable to elevation of privilege.	7.8	More Details
CVE-2023-41372	The vulnerability allows an unprivileged (untrusted) third- party application to arbitrary modify the server settings of the Android Client application, inducing it to connect to an attacker - controlled malicious server.This is possible by forging a valid broadcast intent encrypted with a hardcoded RSA key pair	7.8	More Details
CVE-2023-21373	In Telephony, there is a possible way for a guest user to change the preferred SIM 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.	7.8	More Details
CVE-2023-21355	In libaudioclient, there is a possible out of bounds write due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-3112	A vulnerability was reported in Elliptic Labs Virtual Lock Sensor for ThinkPad T14 Gen 3 that could allow an attacker with local access to execute code with elevated privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21375	In Sysproxy, there is a possible out of bounds write due to an integer underflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-37243	The C:\Windows\Temp\Agent.Package.Availability\Agent.Package.Availability.exe file is automatically launched as SYSTEM when the system reboots. Since the C:\Windows\Temp\Agent.Package.Availability folder inherits permissions from C:\Windows\Temp and Agent.Package.Availability.exe is susceptible to DLL hijacking, standard users can write a malicious DLL to it and elevate their privileges.	7.8	More Details
CVE-2023-21374	In System UI, there is a possible factory reset protection bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-21372	In libdexfile, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2022-3611	An information disclosure vulnerability has been identified in the Lenovo App Store which may allow some applications to gain unauthorized access to sensitive user data used by other unrelated applications.	7.6	More Details
CVE-2023-5044	Code injection via nginx.ingress.kubernetes.io/permanent-redirect annotation.	7.6	More Details
CVE-2023-5043	Ingress nginx annotation injection causes arbitrary command execution.	7.6	More Details
CVE-2023-46376	Zentao Biz version 8.7 and before is vulnerable to Information Disclosure.	7.5	More Details
CVE-2023-46393	gougucms v4.08.18 was discovered to contain a password reset poisoning vulnerability which allows attackers to arbitrarily reset users' passwords via a crafted packet.	7.5	More Details
CVE-2023-40445	The issue was addressed with improved UI handling. This issue is fixed in iOS 17.1 and iPadOS 17.1. A device may persistently fail to lock.	7.5	More Details
CVE-2023-5443	Improper Protection for Outbound Error Messages and Alert Signals vulnerability in EDM Informatics E-invoice allows Account Footprinting.This issue affects E-invoice: before 2.1.	7.5	More Details
CVE-2020-36767	tinyfiledialogs (aka tiny file dialogs) before 3.8.0 allows shell metacharacters in titles, messages, and other input data.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46240	CodeIgniter is a PHP full-stack web framework. Prior to CodeIgniter4 version 4.4.3, if an error or exception occurs, a detailed error report is displayed even if in the production environment. As a result, confidential information may be leaked. Version 4.4.3 contains a patch. As a workaround, replace `ini_set('display_errors', '0')` with `ini_set('display_errors', 'Off')` in `app/Config/Boot/production.php`.	7.5	More Details
CVE-2023-21391	In Messaging, there is a possible way to disable the messaging application due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	7.5	More Details
CVE-2023-39930	A first-factor authentication bypass vulnerability exists in the PingFederate with PingID Radius PCV when a MSCHAP authentication request is sent via a maliciously crafted RADIUS client request.	7.5	More Details
CVE-2023-39619	ReDos in NPMJS Node Email Check v.1.0.4 allows an attacker to cause a denial of service via a crafted string to the scpSyntax component.	7.5	More Details
CVE-2023-46215	Insertion of Sensitive Information into Log File vulnerability in Apache Airflow Celery provider, Apache Airflow. Sensitive information logged as clear text when rediss, amqp, rpc protocols are used as Celery result backend Note: the vulnerability is about the information exposed in the logs not about accessing the logs. This issue affects Apache Airflow Celery provider: from 3.3.0 through 3.4.0; Apache Airflow: from 1.10.0 through 2.6.3. Users are recommended to upgrade Airflow Celery provider to version 3.4.1 and Apache Airlfow to version 2.7.0 which fixes the issue.	7.5	More Details
CVE-2023-27258	Missing authentication in the GetStudentGroupStudents method in IDAttend's IDWeb application 3.1.052 and earlier allows retrieval of student and teacher data by unauthenticated attackers.	7.5	More Details
CVE-2023-5570	Improper Protection for Outbound Error Messages and Alert Signals vulnerability in Inohom Home Manager Gateway allows Account Footprinting.This issue affects Home Manager Gateway: before v.1.27.12.	7.5	More Details
CVE-2015-20110	JHipster generator-jhipster before 2.23.0 allows a timing attack against validateToken due to a string comparison that stops at the first character that is different. Attackers can guess tokens by brute forcing one character at a time and observing the timing. This of course drastically reduces the search space to a linear amount of guesses based on the token length times the possible characters.	7.5	More Details
CVE-2023-27377	Missing authentication in the StudentPopupDetails_EmergencyContactDetails method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction of sensitive student data by unauthenticated attackers.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45899	An issue in the component SuperUserSetuserModuleFrontController:init() of idnovate superuser before v2.4.2 allows attackers to bypass authentication via a crafted HTTP call.	7.5	More Details
CVE-2023-38849	An issue in tire-sales Line v.13.6.1 allows a remote attacker to obtain sensitive information via crafted GET request.	7.5	More Details
CVE-2023-38848	An issue in rmc R Beauty CLINIC Line v.13.6.1 allows a remote attacker to obtain sensitive information via crafted GET request.	7.5	More Details
CVE-2023-38847	An issue in CHRISTINA JAPAN Line v.13.6.1 allows a remote attacker to obtain sensitive information via crafted GET request.	7.5	More Details
CVE-2023-38846	An issue in Marbre Lapin Line v.13.6.1 allows a remote attacker to obtain sensitive information via crafted GET request.	7.5	More Details
CVE-2023-38845	An issue in Anglaise Company Anglaise.Company v.13.6.1 allows a remote attacker to obtain sensitive information via crafted GET request.	7.5	More Details
CVE-2023-27375	Missing authentication in the StudentPopupDetails_ContactDetails method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction of sensitive student data by unauthenticated attackers.	7.5	More Details
CVE-2023-46345	Catdoc v0.95 was discovered to contain a NULL pointer dereference via the component xls2csv at src/xlsparse.c.	7.5	More Details
CVE-2023-21339	In Minikin, there is a possible way to trigger ANR by showing a malicious message due to resource exhaustion. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	7.5	More Details
CVE-2023-5426	The Post Meta Data Manager plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the pmdm_wp_delete_user_meta, pmdm_wp_delete_term_meta, and pmdm_wp_ajax_delete_meta functions in versions up to, and including, 1.2.0. This makes it possible for unauthenticated attackers to delete user, term, and post meta belonging to arbitrary users.	7.5	More Details
CVE-2023-31582	jose4j before v0.9.3 allows attackers to set a low iteration count of 1000 or less.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45955	An issue discovered in Nanoleaf Light strip v3.5.10 allows attackers to cause a denial of service via crafted write binding attribute commands.	7.5	More Details
CVE-2023-37832	A lack of rate limiting in Elenos ETG150 FM transmitter v3.12 allows attackers to obtain user credentials via brute force and cause other unspecified impacts.	7.5	More Details
CVE-2023-27259	Missing authentication in the GetAssignmentsDue method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction of sensitive student and teacher data by unauthenticated attackers.	7.5	More Details
CVE-2023-42488	EisBaer Scada - CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	7.5	More Details
CVE-2023-42847	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. An attacker may be able to access passkeys without authentication.	7.5	More Details
CVE-2023-27257	Missing authentication in the GetActiveToiletPasses method in IDAttend's IDWeb application 3.1.052 and earlier allows retrieval of student information by unauthenticated attackers.	7.5	More Details
CVE-2023-42844	This issue was addressed with improved handling of symlinks. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. A website may be able to access sensitive user data when resolving symlinks.	7.5	More Details
CVE-2023-39219	PingFederate Administrative Console dependency contains a weakness where console becomes unresponsive with crafted Java class loading enumeration requests	7.5	More Details
CVE-2023-46239	quic-go is an implementation of the QUIC protocol in Go. Starting in version 0.37.0 and prior to version 0.37.3, by serializing an ACK frame after the CRYTPO that allows a node to complete the handshake, a remote node could trigger a nil pointer dereference (leading to a panic) when the node attempted to drop the Handshake packet number space. An attacker can bring down a quic-go node with very minimal effort. Completing the QUIC handshake only requires sending and receiving a few packets. Version 0.37.3 contains a patch. Versions before 0.37.0 are not affected.	7.5	More Details
CVE-2023-32359	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 16.7.2 and iPadOS 16.7.2. A user's password may be read aloud by VoiceOver.	7.5	More Details
CVE-2023-42489	EisBaer Scada - CWE-732: Incorrect Permission Assignment for Critical Resource	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5363	Issue summary: A bug has been identified in the processing of key and initialisation vector (IV) lengths. This can lead to potential truncation or overruns during the initialisation of some symmetric ciphers. Impact summary: A truncation in the IV can result in non-uniqueness, which could result in loss of confidentiality for some cipher modes. When calling EVP_EncryptInit_ex2(), EVP_DecryptInit_ex2() or EVP_CipherInit_ex2() the provided OSSL_PARAM array is processed after the key and IV have been established. Any alterations to the key length, via the "keylen" parameter or the IV length, via the "ivlen" parameter, within the OSSL_PARAM array will not take effect as intended, potentially causing truncation or overreading of these values. The following ciphers and cipher modes are impacted: RC2, RC4, RC5, CCM, GCM and OCB. For the CCM, GCM and OCB cipher modes, truncation of the IV can result in loss of confidentiality. For example, when following NIST's SP 800-38D section 8.2.1 guidance for constructing a deterministic IV for AES in GCM mode, truncation of the counter portion could lead to IV reuse. Both truncations and overruns of the key and overruns of the IV will produce incorrect results and could, in some cases, trigger a memory exception. However, these issues are not currently assessed as security critical. Changing the key and/or IV lengths is not considered to be a common operation and the vulnerable API was recently introduced. Furthermore it is likely that application developers will have spotted this problem during testing since decryption would fail unless both peers in the communication were similarly vulnerable. For these reasons we expect the probability of an application being vulnerable to this to be quite low. However if an application is vulnerable then this issue is considered very serious. For these reasons we have assessed this issue as Moderate severity overall. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this because the issue lies outside of the FIPS provider boundary. OpenSSL 3.1 and 3.0 are vulnerable to this issue.	7.5	More Details
CVE-2023-46863	Peppermint Ticket Management before 0.2.4 allows remote attackers to read arbitrary files via a /api/v1/users/file/download?filepath=./../ POST request.	7.5	More Details
CVE-2023-26570	Missing authentication in the StudentPopupDetails_Timetable method in IDAttend’s IDWeb application 3.1.052 and earlier allows extraction sensitive student data by unauthenticated attackers.	7.5	More Details
CVE-2023-4692	An out-of-bounds write flaw was found in grub2's NTFS filesystem driver. This issue may allow an attacker to present a specially crafted NTFS filesystem image, leading to grub's heap metadata corruption. In some circumstances, the attack may also corrupt the UEFI firmware heap metadata. As a result, arbitrary code execution and secure boot protection bypass may be achieved.	7.5	More Details
CVE-2023-4607	An authenticated XCC user can change permissions for any user through a crafted API command.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46129	NATS.io is a high performance open source pub-sub distributed communication technology, built for the cloud, on-premise, IoT, and edge computing. The cryptographic key handling library, nkeys, recently gained support for encryption, not just for signing/authentication. This is used in nats-server 2.10 (Sep 2023) and newer for authentication callouts. In nkeys versions 0.4.0 through 0.4.5, corresponding with NATS server versions 2.10.0 through 2.10.3, the nkeys library's `xkeys` encryption handling logic mistakenly passed an array by value into an internal function, where the function mutated that buffer to populate the encryption key to use. As a result, all encryption was actually to an all-zeros key. This affects encryption only, not signing. FIXME: FILL IN IMPACT ON NATS-SERVER AUTH CALLOUT SECURITY. nkeys Go library 0.4.6, corresponding with NATS Server 2.10.4, has a patch for this issue. No known workarounds are available. For any application handling auth callouts in Go, if using the nkeys library, update the dependency, recompile and deploy that in lockstep.	7.5	More Details
CVE-2023-46662	Sielco PolyEco1000 is vulnerable to an information disclosure vulnerability due to improper access control enforcement. An unauthenticated remote attacker can exploit this via a specially crafted request to gain access to sensitive information.	7.5	More Details
CVE-2023-1356	Reflected cross-site scripting in the StudentSearch component in IDAttend’s IDWeb application 3.1.052 and earlier allows hijacking of a user’s browsing session by attackers who have convinced the said user to click on a malicious link.	7.5	More Details
CVE-2023-21353	In NFA, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	7.5	More Details
CVE-2023-21347	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	7.5	More Details
CVE-2023-31418	An issue has been identified with how Elasticsearch handled incoming requests on the HTTP layer. An unauthenticated user could force an Elasticsearch node to exit with an OutOfMemory error by sending a moderate number of malformed HTTP requests. The issue was identified by Elastic Engineering and we have no indication that the issue is known or that it is being exploited in the wild.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45672	Frigate is an open source network video recorder. Prior to version 0.13.0 Beta 3, an unsafe deserialization vulnerability was identified in the endpoints used to save configurations for Frigate. This can lead to unauthenticated remote code execution. This can be performed through the UI at `/config` or through a direct call to `/api/config/save`. Exploiting this vulnerability requires the attacker to both know very specific information about a user's Frigate server and requires an authenticated user to be tricked into clicking a specially crafted link to their Frigate instance. This vulnerability could exploited by an attacker under the following circumstances: Frigate publicly exposed to the internet (even with authentication); attacker knows the address of a user's Frigate instance; attacker crafts a specialized page which links to the user's Frigate instance; attacker finds a way to get an authenticated user to visit their specialized page and click the button/link. Input is initially accepted through `http.py`. The user-provided input is then parsed and loaded by `load_config_with_no_duplicates`. However, `load_config_with_no_duplicates` does not sanitize this input by merit of using `yaml.loader.Loader` which can instantiate custom constructors. A provided payload will be executed directly at `frigate/util/builtin.py:110`. This issue may lead to pre-authenticated Remote Code Execution. Version 0.13.0 Beta 3 contains a patch.	7.5	More Details
CVE-2023-46119	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Parse Server crashes when uploading a file without extension. This vulnerability has been patched in versions 5.5.6 and 6.3.1.	7.5	More Details
CVE-2023-46346	In the module "Product Catalog (CSV, Excel, XML) Export PRO" (exportproducts) in versions up to 4.1.1 from MyPrestaModules for PrestaShop, a guest can download personal information without restriction by performing a path traversal attack. Due to a lack of permissions control and a lack of control in the path name construction, a guest can perform a path traversal to view all files on the information system.	7.5	More Details
CVE-2023-45670	Frigate is an open source network video recorder. Prior to version 0.13.0 Beta 3, the `config/save` and `config/set` endpoints of Frigate do not implement any CSRF protection. This makes it possible for a request sourced from another site to update the configuration of the Frigate server (e.g. via "drive-by" attack). Exploiting this vulnerability requires the attacker to both know very specific information about a user's Frigate server and requires an authenticated user to be tricked into clicking a specially crafted link to their Frigate instance. This vulnerability could exploited by an attacker under the following circumstances: Frigate publicly exposed to the internet (even with authentication); attacker knows the address of a user's Frigate instance; attacker crafts a specialized page which links to the user's Frigate instance; attacker finds a way to get an authenticated user to visit their specialized page and click the button/link. This issue can lead to arbitrary configuration updates for the Frigate server, resulting in denial of service and possible data exfiltration. Version 0.13.0 Beta 3 contains a patch.	7.5	More Details
CVE-2023-45956	An issue discovered in Govee LED Strip v3.00.42 allows attackers to cause a denial of service via crafted Move and MoveWithOnoff commands.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44397	CloudExplorer Lite is an open source, lightweight cloud management platform. Prior to version 1.4.1, the gateway filter of CloudExplorer Lite uses a controller with path starting with `matching/API/`, which can cause a permission bypass. Version 1.4.1 contains a patch for this issue.	7.5	More Details
CVE-2023-46978	TOTOLINK X6000R V9.4.0cu.852_B20230719 is vulnerable to Incorrect Access Control.Attackers can reset login password & WIFI passwords without authentication.	7.5	More Details
CVE-2023-46289	Rockwell Automation FactoryTalk View Site Edition insufficiently validates user input, which could potentially allow threat actors to send malicious data bringing the product offline. If exploited, the product would become unavailable and require a restart to recover resulting in a denial-of-service condition.	7.5	More Details
CVE-2023-33558	An information disclosure vulnerability in the component users-grid-data.php of Ocomon before v4.0.1 allows attackers to obtain sensitive information such as e-mails and usernames.	7.5	More Details
CVE-2023-26571	Missing authentication in the SetStudentNotes method in IDAttend's IDWeb application 3.1.052 and earlier allows modification of student data by unauthenticated attackers.	7.5	More Details
CVE-2023-5728	During garbage collection extra operations were performed on a object that should not be. This could have led to a potentially exploitable crash. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	7.5	More Details
CVE-2023-42490	EisBaer Scada - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	7.5	More Details
CVE-2023-26580	Unauthenticated arbitrary file read in the IDAttend's IDWeb application 3.1.013 allows the retrieval of any file present on the web server by unauthenticated attackers.	7.5	More Details
CVE-2023-27170	Xpand IT Write-back manager v2.3.1 allows attackers to perform a directory traversal via modification of the siteName parameter.	7.5	More Details
CVE-2023-42494	EisBaer Scada - CWE-749: Exposed Dangerous Method or Function	7.5	More Details
CVE-2023-40401	The issue was addressed with additional permissions checks. This issue is fixed in macOS Ventura 13.6.1. An attacker may be able to access passkeys without authentication.	7.5	More Details
CVE-2023-43905	Incorrect access control in writercms v1.1.0 allows attackers to directly obtain backend account passwords via unspecified vectors.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46992	TOTOLINK A3300R V17.0.0cu.557_B20221024 is vulnerable to Incorrect Access Control. Attackers are able to reset serveral critical passwords without authentication by visiting specific pages.	7.5	More Details
CVE-2023-46852	In Memcached before 1.6.22, a buffer overflow exists when processing multiget requests in proxy mode, if there are many spaces after the "get" substring.	7.5	More Details
CVE-2023-26577	Stored cross-site scripting in the IDAttend's IDWeb application 3.1.052 and earlier allows attackers to hijack the browsing session of the logged in user.	7.5	More Details
CVE-2023-26576	Missing authentication in the SearchStudentsRFID method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction sensitive student data by unauthenticated attackers.	7.5	More Details
CVE-2023-27376	Missing authentication in the StudentPopupDetails_StudentDetails method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction of sensitive student data by unauthenticated attackers.	7.5	More Details
CVE-2018-17559	Due to incorrect access control, unauthenticated remote attackers can view the /video.mjpg video stream of certain ABUS TVIP cameras.	7.5	More Details
CVE-2023-5724	Drivers are not always robust to extremely large draw calls and in some cases this scenario could have led to a crash. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	7.5	More Details
CVE-2023-26575	Missing authentication in the SearchStudentsStaff method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction sensitive student and teacher data by unauthenticated attackers.	7.5	More Details
CVE-2023-26574	Missing authentication in the SearchStudents method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction sensitive student data by unauthenticated attackers.	7.5	More Details
CVE-2023-46664	Sielco PolyEco1000 is vulnerable to an improper access control vulnerability when the application provides direct access to objects based on user-supplied input. As a result of this vulnerability attackers can bypass authorization and access resources behind protected pages.	7.5	More Details
CVE-2023-46663	Sielco PolyEco1000 is vulnerable to an attacker bypassing authorization and accessing resources behind protected pages. The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests.	7.5	More Details
CVE-2023-40685	Management Central as part of IBM i 7.2, 7.3, 7.4, and 7.5 Navigator contains a local privilege escalation vulnerability. A malicious actor with command line access to the operating system can exploit this vulnerability to elevate privileges to gain root access to the operating system. IBM X-Force ID: 264116.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26219	The Hawk Console and Hawk Agent components of TIBCO Software Inc.'s TIBCO Hawk, TIBCO Hawk Distribution for TIBCO Silver Fabric, TIBCO Operational Intelligence Hawk RedTail, and TIBCO Runtime Agent contain a vulnerability that theoretically allows an attacker with access to the Hawk Console's and Agent's log to obtain credentials used to access associated EMS servers. Affected releases are TIBCO Software Inc.'s TIBCO Hawk: versions 6.2.2 and below, TIBCO Hawk Distribution for TIBCO Silver Fabric: versions 6.2.2 and below, TIBCO Operational Intelligence Hawk RedTail: versions 7.2.1 and below, and TIBCO Runtime Agent: versions 5.12.2 and below.	7.4	More Details
CVE-2023-34059	open-vm-tools contains a file descriptor hijack vulnerability in the vmware-user-suid-wrapper. A malicious actor with non-root privileges may be able to hijack the /dev/uinput file descriptor allowing them to simulate user inputs.	7.4	More Details
CVE-2023-45780	In Print Service, there is a possible background activity launch due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.3	More Details
CVE-2023-5780	A vulnerability classified as critical was found in Tongda OA 2017 11.10. This vulnerability affects unknown code of the file general/system/approve_center/flow_guide/flow_type/set_print/delete.php. The manipulation of the argument DELETE_STR leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-243586 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2023-5804	A vulnerability was found in PHPGurukul Nipah Virus Testing Management System 1.0 and classified as critical. This issue affects some unknown processing of the file login.php. The manipulation of the argument username leads to sql injection. The attack may be initiated remotely. The identifier VDB-243617 was assigned to this vulnerability.	7.3	More Details
CVE-2023-5787	A vulnerability was found in Shaanxi Chanming Education Technology Score Query System 5.0. It has been rated as critical. This issue affects some unknown processing. The manipulation of the argument stuIdCard 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-243593 was assigned to this vulnerability.	7.3	More Details
CVE-2023-39231	PingFederate using the PingOne MFA adapter allows a new MFA device to be paired without requiring second factor authentication from an existing registered device. A threat actor may be able to exploit this vulnerability to register their own MFA device if they have knowledge of a victim user's first factor credentials.	7.3	More Details
CVE-2023-5794	A vulnerability was found in PHPGurukul Online Railway Catering System 1.0. It has been classified as critical. Affected is an unknown function of the file index.php of the component Login. The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-243600.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5828	A vulnerability was found in Nanning Ontall Longxing Industrial Development Zone Project Construction and Installation Management System up to 20231026. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file login.aspx. The manipulation of the argument tbxUserName 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-243727.	7.3	More Details
CVE-2023-5830	A vulnerability classified as critical has been found in ColumbiaSoft Document Locator. This affects an unknown part of the file /api/authentication/login of the component WebTools. The manipulation of the argument Server leads to improper authentication. It is possible to initiate the attack remotely. Upgrading to version 7.2 SP4 and 2021.1 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-243729 was assigned to this vulnerability.	7.3	More Details
CVE-2023-44220	SonicWall NetExtender Windows (32-bit and 64-bit) client 10.2.336 and earlier versions have a DLL Search Order Hijacking vulnerability in the start-up DLL component. Successful exploitation via a local attacker could result in command execution in the target system.	7.3	More Details
CVE-2023-3010	Grafana is an open-source platform for monitoring and observability. The WorldMap panel plugin, versions before 1.0.4 contains a DOM XSS vulnerability.	7.3	More Details
CVE-2023-25047	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in David F. Carr RSVPMaker rsvpmaker allows SQL Injection.This issue affects RSVPMaker: from n/a through 9.9.3.	7.2	More Details
CVE-2023-5624	Under certain conditions, Nessus Network Monitor was found to not properly enforce input validation. This could allow an admin user to alter parameters that could potentially allow a blindSQL injection.	7.2	More Details
CVE-2023-20273	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	7.2	More Details
CVE-2023-46865	/api/v1/company/upload-logo in CompanyController.php in crater through 6.0.6 allows a superadmin to execute arbitrary PHP code by placing this code into an image/png IDAT chunk of a Company Logo image.	7.2	More Details
CVE-2023-46818	An issue was discovered in ISPConfig before 3.2.11p1. PHP code injection can be achieved in the language file editor by an admin if admin_allow_langedit is enabled.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45799	In MLSoft TCO!stream versions 8.0.22.1115 and below, a vulnerability exists due to insufficient permission validation. This allows an attacker to make the victim download and execute arbitrary files.	7.2	More Details
CVE-2023-5844	Unverified Password Change in GitHub repository pimcore/admin-ui-classic-bundle prior to 1.2.0.	7.2	More Details
CVE-2023-43507	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance. An attacker could exploit this vulnerability to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the ClearPass Policy Manager cluster.	7.2	More Details
CVE-2023-30912	A remote code execution issue exists in HPE OneView.	7.2	More Details
CVE-2023-46245	Kimai is a web-based multi-user time-tracking application. Versions prior to 2.1.0 are vulnerable to a Server-Side Template Injection (SSTI) which can be escalated to Remote Code Execution (RCE). The vulnerability arises when a malicious user uploads a specially crafted Twig file, exploiting the software's PDF and HTML rendering functionalities. Version 2.1.0 enables security measures for custom Twig templates.	7.2	More Details
CVE-2023-42493	EisBaer Scada - CWE-256: Plaintext Storage of a Password	7.1	More Details
CVE-2023-45769	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Alex Raven WP Report Post plugin <= 2.1.2 versions.	7.1	More Details
CVE-2023-46209	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in G5Theme Grid Plus – Unlimited grid plugin <= 1.3.2 versions.	7.1	More Details
CVE-2023-34058	VMware Tools contains a SAML token signature bypass vulnerability. A malicious actor that has been granted Guest Operation Privileges https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-security/GUID-6A952214-0E5E-4CCF-9D2A-90948FF643EC.html in a target virtual machine may be able to elevate their privileges if that target virtual machine has been assigned a more privileged Guest Alias https://vdc-download.vmware.com/vmwb-repository/dcr-public/d1902b0e-d479-46bf-8ac9-cee0e31e8ec0/07ce8dbd-db48-4261-9b8f-c6d3ad8ba472/vim.vm.guest.AliasManager.html .	7.1	More Details
CVE-2023-5622	Under certain conditions, Nessus Network Monitor could allow a low privileged user to escalate privileges to NT AUTHORITY\SYSTEM on Windows hosts by replacing a specially crafted file.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46208	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in StylemixThemes Motors – Car Dealer, Classifieds & Listing plugin <= 1.4.6 versions.	7.1	More Details
CVE-2023-46071	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in ClickDatos Protección de Datos RGPD plugin <= 3.1.0 versions.	7.1	More Details
CVE-2023-46070	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Emmanuel GEORJON EG-Attachments plugin <= 2.1.3 versions.	7.1	More Details
CVE-2023-46622	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in ollybach WPPizza – A Restaurant Plugin plugin <= 3.18.2 versions.	7.1	More Details
CVE-2023-46313	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Katie Seaborn Zotpress plugin <= 7.3.4 versions.	7.1	More Details
CVE-2023-46312	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Zaytech Smart Online Order for Clover plugin <= 1.5.4 versions.	7.1	More Details
CVE-2023-45837	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in XYDAC Ultimate Taxonomy Manager plugin <= 2.0 versions.	7.1	More Details
CVE-2023-45835	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Libsyn Libsyn Publisher Hub plugin <= 1.4.4 versions.	7.1	More Details
CVE-2023-42492	EisBaer Scada - CWE-321: Use of Hard-coded Cryptographic Key	7.1	More Details
CVE-2023-45770	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Fastwpspeed Fast WP Speed plugin <= 1.0.0 versions.	7.1	More Details
CVE-2023-45772	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Scribit Proofreading plugin <= 1.0.11 versions.	7.1	More Details
CVE-2023-46153	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in UserFeedback Team User Feedback plugin <= 1.0.9 versions.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45750	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in POSIMYTH Nexter Extension plugin <= 2.0.3 versions.	7.1	More Details
CVE-2023-46075	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in wpdevart Contact Form Builder, Contact Widget plugin <= 2.1.6 versions.	7.1	More Details
CVE-2023-46076	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in RedNao WooCommerce PDF Invoice Builder, Create invoices, packing slips and more plugin <= 1.2.102 versions.	7.1	More Details
CVE-2023-46077	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Arrow Plugins The Awesome Feed – Custom Feed plugin <= 2.2.5 versions.	7.1	More Details
CVE-2023-46081	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in Lavacode Lava Directory Manager plugin <= 1.1.34 versions.	7.1	More Details
CVE-2023-45637	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in EventPrime EventPrime – Events Calendar, Bookings and Tickets plugin <= 3.1.5 versions.	7.1	More Details
CVE-2023-45761	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Joovii Sendle Shipping Plugin plugin <= 5.13 versions.	7.1	More Details
CVE-2023-46094	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Conversios Track Google Analytics 4, Facebook Pixel & Conversions API via Google Tag Manager for WooCommerce plugin <= 6.5.3 versions.	7.1	More Details
CVE-2023-46072	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Michael Simpson Add Shortcodes Actions And Filters plugin <= 2.0.9 versions.	7.1	More Details
CVE-2023-41960	The vulnerability allows an unprivileged(untrusted) third-party application to interact with a content-provider unsafely exposed by the Android Agent application, potentially modifying sensitive settings of the Android Client application itself.	7.1	More Details
CVE-2023-46090	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WebDorado WDSocialWidgets plugin <= 1.0.15 versions.	7.1	More Details
CVE-2023-45759	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Peter Keung Peter's Custom Anti-Spam plugin <= 3.2.2 versions.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45756	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Spider Teams ApplyOnline – Application Form Builder and Manager plugin <= 2.5.2 versions.	7.1	More Details
CVE-2023-38041	A logged in user may elevate its permissions by abusing a Time-of-Check to Time-of-Use (TOCTOU) race condition. When a particular process flow is initiated, an attacker can exploit this condition to gain unauthorized elevated privileges on the affected system.	7.0	More Details
CVE-2023-40131	In GpuService of GpuService.cpp, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.0	More Details
CVE-2023-5623	NNM failed to properly set ACLs on its installation directory, which could allow a low privileged user to run arbitrary code with SYSTEM privileges where NNM is installed to a non-standard location	7.0	More Details
CVE-2023-5574	A use-after-free flaw was found in xorg-x11-server-Xvfb. This issue occurs in Xvfb with a very specific and legacy configuration (a multi-screen setup with multiple protocol screens, also known as Zaphod mode). If the pointer is warped from a screen 1 to a screen 0, a use-after-free issue may be triggered during shutdown or reset of the Xvfb server, allowing for possible escalation of privileges or denial of service.	7.0	More Details
CVE-2023-46813	An issue was discovered in the Linux kernel before 6.5.9, exploitable by local users with userspace access to MMIO registers. Incorrect access checking in the #VC handler and instruction emulation of the SEV-ES emulation of MMIO accesses could lead to arbitrary write access to kernel memory (and thus privilege escalation). This depends on a race condition through which userspace can replace an instruction before the #VC handler reads it.	7.0	More Details
CVE-2023-41096	Missing Encryption of Security Keys vulnerability in Silicon Labs Ember ZNet SDK on 32 bit, ARM (SecureVault High modules) allows potential modification or extraction of network credentials stored in flash. This issue affects Silicon Labs Ember ZNet SDK: 7.3.1 and earlier.	6.8	More Details
CVE-2023-41095	Missing Encryption of Security Keys vulnerability in Silicon Labs OpenThread SDK on 32 bit, ARM (SecureVault High modules) allows potential modification or extraction of network credentials stored in flash. This issue affects Silicon Labs OpenThread SDK: 2.3.1 and earlier.	6.8	More Details
CVE-2023-41988	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data.	6.8	More Details
CVE-2023-45844	The vulnerability allows a low privileged user that have access to the device when locked in Kiosk mode to install an arbitrary Android application and leverage it to have access to critical device settings such as the device power management or eventually the device secure settings (ADB debug).	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41989	The issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1. An attacker may be able to execute arbitrary code as root from the Lock Screen.	6.8	More Details
CVE-2022-4573	An SMI handler input validation vulnerability in the ThinkPad X1 Fold Gen 1 could allow an attacker with local access and elevated privileges to execute arbitrary code.	6.7	More Details
CVE-2023-25045	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in David F. Carr RSVPMaker allows SQL Injection.This issue affects RSVPMaker: from n/a through 9.9.3.	6.7	More Details
CVE-2022-4574	An SMI handler input validation vulnerability in the BIOS of some ThinkPad models could allow an attacker with local access and elevated privileges to execute arbitrary code.	6.7	More Details
CVE-2022-4575	A vulnerability due to improper write protection of UEFI variables was reported in the BIOS of some ThinkPad models could allow an attacker with physical or local access and elevated privileges the ability to bypass Secure Boot.	6.7	More Details
CVE-2023-21310	In Bluetooth, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	6.7	More Details
CVE-2023-21360	In Bluetooth, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	6.7	More Details
CVE-2022-48189	An SMM driver input validation vulnerability in the BIOS of some ThinkPad models could allow an attacker with local access and elevated privileges to execute arbitrary code.	6.7	More Details
CVE-2023-21380	In Bluetooth, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	6.7	More Details
CVE-2023-21371	In Secure Element, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	6.7	More Details
CVE-2023-21370	In the Security Element API, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42849	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An attacker that has already achieved kernel code execution may be able to bypass kernel memory mitigations.	6.5	More Details
CVE-2023-45640	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in TechnoWich WP ULike – Most Advanced WordPress Marketing Toolkit plugin <= 4.6.8 versions.	6.5	More Details
CVE-2023-21395	In Bluetooth, there is a possible out of bounds read due to a use after free. This could lead to remote information disclosure over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.	6.5	More Details
CVE-2023-45829	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in HappyBox Newsletter & Bulk Email Sender – Email Newsletter Plugin for WordPress plugin <= 2.0.1 versions.	6.5	More Details
CVE-2023-31419	A flaw was discovered in Elasticsearch, affecting the _search API that allowed a specially crafted query string to cause a Stack Overflow and ultimately a Denial of Service.	6.5	More Details
CVE-2023-40416	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. Processing an image may result in disclosure of process memory.	6.5	More Details
CVE-2023-46128	Nautobot is a Network Automation Platform built as a web application atop the Django Python framework with a PostgreSQL or MySQL database. In Nautobot 2.0.x, certain REST API endpoints, in combination with the `?depth=<N>` query parameter, can expose hashed user passwords as stored in the database to any authenticated user with access to these endpoints. The passwords are not exposed in plaintext. This vulnerability has been patched in version 2.0.3.	6.5	More Details
CVE-2022-3429	A denial-of-service vulnerability was found in the firmware used in Lenovo printers, where users send illegal or malformed strings to an open port, triggering a denial of service that causes a display error and prevents the printer from functioning properly.	6.5	More Details
CVE-2023-46361	Artifex Software jbig2dec v0.20 was discovered to contain a SEGV vulnerability via jbig2_error at /jbig2dec/jbig2.c.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46125	Fides is an open-source privacy engineering platform for managing the fulfillment of data privacy requests in a runtime environment, and the enforcement of privacy regulations in code. The Fides webserver API allows users to retrieve its configuration using the `GET api/v1/config` endpoint. The configuration data is filtered to suppress most sensitive configuration information before it is returned to the user, but even the filtered data contains information about the internals and the backend infrastructure, such as various settings, servers' addresses and ports and database username. This information is useful for administrative users as well as attackers, thus it should not be revealed to low-privileged users. This vulnerability allows Admin UI users with roles lower than the owner role e.g. the viewer role to retrieve the config information using the API. The vulnerability has been patched in Fides version `2.22.1`.	6.5	More Details
CVE-2023-43041	IBM QRadar SIEM 7.5 is vulnerable to information exposure allowing a delegated Admin tenant user with a specific domain security profile assigned to see data from other domains. This vulnerability is due to an incomplete fix for CVE-2022-34352. IBM X-Force ID: 266808.	6.5	More Details
CVE-2023-46069	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Osmansorkar Ajax Archive Calendar plugin <= 2.6.7 versions.	6.5	More Details
CVE-2023-46866	In International Color Consortium DemoIccMAX 79ecb74, CIccCLUT::Interp3d in IccProfLib/IccTagLut.cpp in libSampleICC.a attempts to access array elements at out-of-bounds indexes.	6.5	More Details
CVE-2022-3681	A vulnerability has been identified in the MR2600 router v1.0.18 and earlier that could allow an attacker within range of the wireless network to successfully brute force the WPS pin, potentially allowing them unauthorized access to a wireless network.	6.5	More Details
CVE-2023-41983	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.1, Safari 17.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. Processing web content may lead to a denial-of-service.	6.5	More Details
CVE-2023-42861	A logic issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.1. An attacker with knowledge of a standard user's credentials can unlock another standard user's locked screen on the same Mac.	6.5	More Details
CVE-2023-45646	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Henryholtgeerts PDF Block plugin <= 1.1.0 versions.	6.5	More Details
CVE-2023-46867	In International Color Consortium DemoIccMAX 79ecb74, CIccXformMatrixTRC::GetCurve in IccCmm.cpp in libSampleICC.a has a NULL pointer dereference.	6.5	More Details
CVE-2023-30492	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Vark Minimum Purchase for WooCommerce plugin <= 2.0.0.1 versions.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39610	An issue in TP-Link Tapo C100 v1.1.15 Build 211130 Rel.15378n(4555) and before allows attackers to cause a Denial of Service (DoS) via supplying a crafted web request.	6.5	More Details
CVE-2023-46653	Jenkins lambdatest-automation Plugin 1.20.10 and earlier logs LAMBDATEST Credentials access token at the INFO level, potentially resulting in its exposure.	6.5	More Details
CVE-2023-41966	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter.	6.5	More Details
CVE-2022-38485	A directory traversal vulnerability exists in the AgeVolt Portal prior to version 0.1 that leads to Information Disclosure. A remote authenticated attacker could leverage this vulnerability to read files from any location on the target operating system with web server privileges.	6.5	More Details
CVE-2023-5727	The executable file warning was not presented when downloading .msix, .msixbundle, .appx, and .appxbundle files, which can run commands on a user's computer. *Note: This issue only affected Windows operating systems. Other operating systems are unaffected.* This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	6.5	More Details
CVE-2023-46234	browserify-sign is a package to duplicate the functionality of node's crypto public key functions, much of this is based on Fedor Indutny's work on indutny/tls.js. An upper bound check issue in `dsaVerify` function allows an attacker to construct signatures that can be successfully verified by any public key, thus leading to a signature forgery attack. All places in this project that involve DSA verification of user-input signatures will be affected by this vulnerability. This issue has been patched in version 4.2.2.	6.5	More Details
CVE-2023-45867	ILIAS (2013-09-12 release) contains a medium-criticality Directory Traversal local file inclusion vulnerability in the ScormAicc module. An attacker with a privileged account, typically holding the tutor role, can exploit this to gain unauthorized access to and potentially retrieve confidential files stored on the web server. The attacker can access files that are readable by the web server user www-data; this may include sensitive configuration files and documents located outside the documentRoot. The vulnerability is exploited by an attacker who manipulates the file parameter in a URL, inserting directory traversal sequences in order to access unauthorized files. This manipulation allows the attacker to retrieve sensitive files, such as /etc/passwd, potentially compromising the system's security. This issue poses a significant risk to confidentiality and is remotely exploitable over the internet.	6.5	More Details
CVE-2022-34832	An issue was discovered in VERMEG AgileReporter 21.3. XXE can occur via an XML document to the Analysis component.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46490	SQL Injection vulnerability in Cacti v1.2.25 allows a remote attacker to obtain sensitive information via the form_actions() function in the managers.php function.	6.5	More Details
CVE-2023-46655	Jenkins CloudBees CD Plugin 1.1.32 and earlier follows symbolic links to locations outside of the directory from which artifacts are published during the 'CloudBees CD - Publish Artifact' post-build step, allowing attackers able to configure jobs to publish arbitrary files from the Jenkins controller file system to the previously configured CloudBees CD server.	6.5	More Details
CVE-2023-37911	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Starting in version 9.4-rc-1 and prior to versions 14.10.8 and 15.3-rc-1, when a document has been deleted and re-created, it is possible for users with view right on the re-created document but not on the deleted document to view the contents of the deleted document. Such a situation might arise when rights were added to the deleted document. This can be exploited through the diff feature and, partially, through the REST API by using versions such as `deleted:1` (where the number counts the deletions in the wiki and is thus guessable). Given sufficient rights, the attacker can also re-create the deleted document, thus extending the scope to any deleted document as long as the attacker has edit right in the location of the deleted document. This vulnerability has been patched in XWiki 14.10.8 and 15.3 RC1 by properly checking rights when deleted revisions of a document are accessed. The only workaround is to regularly clean deleted documents to minimize the potential exposure. Extra care should be taken when deleting sensitive documents that are protected individually (and not, e.g., by being placed in a protected space) or deleting a protected space as a whole.	6.5	More Details
CVE-2023-5732	An attacker could have created a malicious link using bidirectional characters to spoof the location in the address bar when visited. This vulnerability affects Firefox < 117, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	6.5	More Details
CVE-2023-46651	Jenkins Warnings Plugin 10.5.0 and earlier does not set the appropriate context for credentials lookup, allowing attackers with Item/Configure permission to access and capture credentials they are not entitled to. This fix has been backported to 10.4.1.	6.5	More Details
CVE-2020-17477	Incorrect LDAP ACLs in ucs-school-ldap-acls-master in UCS@school before 4.4v5-errata allow remote teachers, staff, and school administrators to read LDAP password hashes (sambaNTPassword, krb5Key, sambaPasswordHistory, and pwhistory) via LDAP search requests. For example, a teacher can gain administrator access via an NTLM hash.	6.5	More Details
CVE-2023-21315	In Bluetooth, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote (proximal/adjacent) information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	6.5	More Details
CVE-2023-43281	Double Free vulnerability in Nothings Stb Image.h v.2.28 allows a remote attacker to cause a denial of service via a crafted file to the stbi_load_gif_main function.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42188	IceCMS v2.0.1 is vulnerable to Cross Site Request Forgery (CSRF).	6.5	More Details
CVE-2023-46211	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Brainstorm Force Ultimate Addons for WPBakery Page Builder plugin <= 3.19.14 versions.	6.5	More Details
CVE-2023-47090	NATS nats-server before 2.9.23 and 2.10.x before 2.10.2 has an authentication bypass. An implicit $G user in an authorization block can sometimes be used for unauthenticated access, even when the intention of the configuration was for each user to have an account. The earliest affected version is 2.2.0.	6.5	More Details
CVE-2023-45228	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters.	6.5	More Details
CVE-2023-5127	The WP Font Awesome plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 1.7.9 due to insufficient input sanitization and output escaping on 'icon' user supplied attribute. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5116	The Live updates from Excel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ipushpull_page' shortcode in versions up to, and including, 2.3.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5740	The Live Chat with Facebook Messenger plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'messenger' shortcode in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5744	The Very Simple Google Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'vsgmap' shortcode in all versions up to, and including, 2.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5073	The iframe forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'iframe' shortcode in versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5705	The VK Filter Search plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'vk_filter_search' shortcode in all versions up to, and including, 2.3.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5774	The Animated Counters plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 1.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5817	The Neon text plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's neontext_box shortcode in all versions up to, and including, 1.1 due to insufficient input sanitization and output escaping on user supplied attributes (color). This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5250	The Grid Plus plugin for WordPress is vulnerable to Local File Inclusion in versions up to, and including, 1.3.2 via a shortcode attribute. This allows subscriber-level, and above, attackers to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where PHP files with arbitrary content can be uploaded and included. This is limited to .php files.	6.4	More Details
CVE-2023-5666	The Accordion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'tcpaccordion' shortcode in all versions up to, and including, 2.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5566	The Simple Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 1.0.20 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5565	The Shortcode Menu plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'shortmenu' shortcode in versions up to, and including, 3.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5362	The Carousel, Recent Post Slider and Banner Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'spice_post_slider' shortcode in versions up to, and including, 2.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5335	The Buzzsprout Podcasting plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'buzzsprout' shortcode in versions up to, and including, 1.8.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5252	The FareHarbor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 3.6.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5085	The Advanced Menu Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'advMenu' shortcode in versions up to, and including, 0.4.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5164	The Bellows Accordion Menu plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 1.4.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5049	The Giveaways and Contests by RafflePress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'rafflepress' and 'rafflepress_gutenberg' shortcode in versions up to, and including, 1.12.0 due to insufficient input sanitization and output escaping on 'giframe' user supplied attribute. This makes it possible for authenticated attackers with contributor level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5051	The CallRail Phone Call Tracking plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'callrail_form' shortcode in versions up to, and including, 0.5.2 due to insufficient input sanitization and output escaping on the 'form_id' user supplied attribute. This makes it possible for authenticated attackers with contributor level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5110	The BSK PDF Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'bsk-pdfm-category-dropdown' shortcode in versions up to, and including, 3.4.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-43508	Vulnerabilities in the web-based management interface of ClearPass Policy Manager allow an attacker with read-only privileges to perform actions that change the state of the ClearPass Policy Manager instance. Successful exploitation of these vulnerabilities allow an attacker to complete state-changing actions in the web-based management interface that should not be allowed by their current level of authorization on the platform.	6.3	More Details
CVE-2023-5805	A vulnerability was found in SourceCodester Simple Real Estate Portal System 1.0. It has been classified as critical. Affected is an unknown function of the file view_estate.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-243618 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-43797	BigBlueButton is an open-source virtual classroom. Prior to versions 2.6.11 and 2.7.0-beta.3, Guest Lobby was vulnerable to cross-site scripting when users wait to enter the meeting due to inserting unsanitized messages to the element using unsafe innerHTML. Text sanitizing was added for lobby messages starting in versions 2.6.11 and 2.7.0-beta.3. There are no known workarounds.	6.3	More Details
CVE-2023-5792	A vulnerability has been found in SourceCodester Sticky Notes App 1.0 and classified as critical. This vulnerability affects unknown code of the file endpoint/delete-note.php. The manipulation of the argument note leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-243598 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-5795	A vulnerability was found in CodeAstro POS System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /profil of the component Profile Picture Handler. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-243601 was assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5796	A vulnerability was found in CodeAstro POS System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /setting of the component Logo Handler. The manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-243602 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-5790	A vulnerability classified as critical was found in SourceCodester File Manager App 1.0. Affected by this vulnerability is an unknown functionality of the file endpoint/add-file.php. The manipulation of the argument uploadedFileName leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-243595.	6.3	More Details
CVE-2023-5783	A vulnerability has been found in Tongda OA 2017 up to 11.9 and classified as critical. Affected by this vulnerability is an unknown functionality of the file general/system/approve_center/flow_sort/flow/delete.php. The manipulation of the argument id/sort_parent leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-243589 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-5829	A vulnerability was found in code-projects Admission Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file student_avatar.php. The manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-243728.	6.3	More Details
CVE-2023-5781	A vulnerability, which was classified as critical, has been found in Tongda OA 2017 11.10. This issue affects the function DELETE_STR of the file general/system/res_manage/monitor/delete_webmail.php. The manipulation 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-243587. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-5753	Potential buffer overflows in the Bluetooth subsystem due to asserts being disabled in /subsys/bluetooth/host/hci_core.c	6.3	More Details
CVE-2023-5836	A vulnerability was found in SourceCodester Task Reminder System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file classes/Users.php?f=delete. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The identifier of this vulnerability is VDB-243800.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2007-10003	A vulnerability, which was classified as critical, has been found in The Hackers Diet Plugin up to 0.9.6b on WordPress. This issue affects some unknown processing of the file ajax_blurb.php of the component HTTP POST Request Handler. The manipulation of the argument user leads to sql injection. The attack may be initiated remotely. Upgrading to version 0.9.7b is able to address this issue. The patch is named 7dd8acf7cd844260984003712107 4425d363b694. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-243803.	6.3	More Details
CVE-2023-5813	A vulnerability was found in SourceCodester Task Reminder System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /classes/Master.php?f=delete_reminder. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The identifier of this vulnerability is VDB-243644.	6.3	More Details
CVE-2021-33634	iSulad uses the lcr+lxc runtime (default) to run malicious images, which can cause DOS.	6.3	More Details
CVE-2023-5814	A vulnerability was found in SourceCodester Task Reminder System 1.0. It has been classified as critical. This affects an unknown part of the file /classes/Master.php?f=save_reminder. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The identifier VDB-243645 was assigned to this vulnerability.	6.3	More Details
CVE-2023-46722	The Pimcore Admin Classic Bundle provides a backend UI for Pimcore. Prior to version 1.2.0, a cross-site scripting vulnerability has the potential to steal a user's cookie and gain unauthorized access to that user's account through the stolen cookie or redirect users to other malicious sites. Users should upgrade to version 1.2.0 to receive a patch or, as a workaround, apply the patch manually.	6.1	More Details
CVE-2023-36085	The sisqualWFM 7.1.319.103 thru 7.1.319.111 for Android, has a host header injection vulnerability in its "/sisqualIdentityServer/core/" endpoint. By modifying the HTTP Host header, an attacker can change webpage links and even redirect users to arbitrary or malicious locations. This can lead to phishing attacks, malware distribution, and unauthorized access to sensitive resources.	6.1	More Details
CVE-2023-36920	In SAP Enable Now - versions WPB_MANAGER 1.0, WPB_MANAGER_CE 10, WPB_MANAGER_HANA 10, ENABLE_NOW_CONSUMP_DEL 1704, the X-FRAME-OPTIONS response header is not implemented, allowing an unauthenticated attacker to attempt clickjacking, which could result in disclosure or modification of information.	6.1	More Details
CVE-2023-44484	Online Blood Donation Management System v1.0 is vulnerable to a Stored Cross-Site Scripting vulnerability. The 'firstName' parameter of the users/register.php resource is copied into the users/member.php document as plain text between tags. Any input is echoed unmodified in the users/member.php response.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5211	The Fattura24 WordPress plugin before 6.2.8 does not sanitize or escape the 'id' parameter before outputting it back in the page, leading to a reflected Cross-Site Scripting vulnerability.	6.1	More Details
CVE-2023-5238	The EventPrime WordPress plugin before 3.2.0 does not sanitise and escape a parameter before outputting it back in the page, leading to an HTML Injection on the plugin in the search area of the website.	6.1	More Details
CVE-2023-5307	The Photos and Files Contest Gallery WordPress plugin before 21.2.8.1 does not sanitise and escape some parameters, which could allow unauthenticated users to perform Cross-Site Scripting attacks via certain headers.	6.1	More Details
CVE-2023-4250	The EventPrime WordPress plugin before 3.2.0 does not sanitise and escape some parameters before outputting them back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin.	6.1	More Details
CVE-2023-43906	Xolo CMS v0.11 was discovered to contain a reflected cross-site scripting (XSS) vulnerability.	6.1	More Details
CVE-2023-43647	baserCMS is a website development framework. Prior to version 4.8.0, there is a cross-site scripting vulnerability in the file upload feature of baserCMS. Version 4.8.0 contains a patch for this issue.	6.1	More Details
CVE-2023-46134	D-Tale is the combination of a Flask back-end and a React front-end to view & analyze Pandas data structures. Prior to version 3.7.0, users hosting D-Tale publicly can be vulnerable to remote code execution, allowing attackers to run malicious code on the server. This issue has been patched in version 3.7.0 by turning off "Custom Filter" input by default. The only workaround for versions earlier than 3.7.0 is to only host D-Tale to trusted users.	6.1	More Details
CVE-2023-46583	Cross-Site Scripting (XSS) vulnerability in PHPGurukul Nipah virus (NiV) " Testing Management System v.1.0 allows attackers to execute arbitrary code via a crafted payload injected into the State field.	6.1	More Details
CVE-2023-46503	Cross Site Scripting (XSS) vulnerability in PwnCYN YXBOOKCMS v.1.0.2 allows a remote attacker to execute arbitrary code via the reader management and book input modules.	6.1	More Details
CVE-2023-46505	Cross Site Scripting vulnerability in FanCMS v.1.0.0 allows an attacker to execute arbitrary code via the content1 parameter in the demo.php file.	6.1	More Details
CVE-2023-5758	When opening a page in reader mode, the redirect URL could have caused attacker-controlled script to execute in a reflected Cross-Site Scripting (XSS) attack. This vulnerability affects Firefox for iOS < 119.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3700	A Time of Check Time of Use (TOCTOU) vulnerability was reported in the Lenovo Vantage SystemUpdate Plugin version 2.0.0.212 and earlier that could allow a local attacker to delete arbitrary files.	6.1	More Details
CVE-2023-46491	ZenTao Biz version 4.1.3 and before has a Cross Site Scripting (XSS) vulnerability in the Version Library.	6.1	More Details
CVE-2022-3702	A denial of service vulnerability was reported in Lenovo Vantage HardwareScan Plugin version 1.3.0.5 and earlier that could allow a local attacker to delete contents of an arbitrary directory under certain conditions.	6.1	More Details
CVE-2023-29009	baserCMS is a website development framework with WebAPI that runs on PHP8 and CakePHP4. There is a XSS Vulnerability in Favorites Feature to baserCMS. This issue has been patched in version 4.8.0.	6.1	More Details
CVE-2023-46374	ZenTao Enterprise Edition version 4.1.3 and before is vulnerable to Cross Site Scripting (XSS).	6.1	More Details
CVE-2023-5863	Cross-site Scripting (XSS) - Reflected in GitHub repository thorsten/phpmyfaq prior to 3.2.2.	6.1	More Details
CVE-2023-32738	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Alkaweb Eonet Manual User Approve plugin <= 2.1.3 versions.	5.9	More Details
CVE-2023-45764	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Gopi Ramasamy Scroll post excerpt plugin <= 8.0 versions.	5.9	More Details
CVE-2023-25032	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Print, PDF, Email by PrintFriendly plugin <= 5.5.1 versions.	5.9	More Details
CVE-2023-45747	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Syed Balkhi WP Lightbox 2 plugin <= 3.0.6.5 versions.	5.9	More Details
CVE-2023-45754	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in I Thirteen Web Solution Easy Testimonial Slider and Form allows Stored XSS.This issue affects Easy Testimonial Slider and Form: from n/a through 1.0.18.	5.9	More Details
CVE-2023-45755	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in BuddyBoss BuddyPress Global Search plugin <= 1.2.1 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45758	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Marco Milesi Amministrazione Trasparente plugin <= 8.0.2 versions.	5.9	More Details
CVE-2023-46068	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in XQueue GmbH Maileon for WordPress plugin <= 2.16.0 versions.	5.9	More Details
CVE-2023-46210	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WebCource WC Captcha plugin <= 1.4 versions.	5.9	More Details
CVE-2015-0897	LINE for Android version 5.0.2 and earlier and LINE for iOS version 5.0.0 and earlier are vulnerable to MITM (man-in-the-middle) attack since the application allows non-SSL/TLS communications. As a result, any API may be invoked from a script injected by a MITM (man-in-the-middle) attacker.	5.9	More Details
CVE-2023-46091	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Bala Krishna, Sergey Yakovlev Category SEO Meta Tags plugin <= 2.5 versions.	5.9	More Details
CVE-2023-45833	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in LeadSquared Suite plugin <= 0.7.4 versions.	5.9	More Details
CVE-2023-45832	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Martin Gibson WP GoToWebinar plugin <= 14.45 versions.	5.9	More Details
CVE-2023-46199	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Triberr plugin <= 4.1.1 versions.	5.9	More Details
CVE-2023-46192	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Internet Marketing Ninjas Internal Link Building plugin <= 1.2.3 versions.	5.9	More Details
CVE-2023-45768	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Stephanie Leary Next Page plugin <= 1.5.2 versions.	5.9	More Details
CVE-2023-5568	A heap-based Buffer Overflow flaw was discovered in Samba. It could allow a remote, authenticated attacker to exploit this vulnerability to cause a denial of service.	5.9	More Details
CVE-2023-45644	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Anurag Deshmukh CPT Shortcode Generator plugin <= 1.0 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31421	It was discovered that when acting as TLS clients, Beats, Elastic Agent, APM Server, and Fleet Server did not verify whether the server certificate is valid for the target IP address; however, certificate signature validation is still performed. More specifically, when the client is configured to connect to an IP address (instead of a hostname) it does not validate the server certificate's IP SAN values against that IP address and certificate validation fails, and therefore the connection is not blocked as expected.	5.9	More Details
CVE-2023-40681	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Groundhogg Inc. Groundhogg plugin <= 2.7.11.10 versions.	5.9	More Details
CVE-2023-46200	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Stephen Darlington, Wandle Software Limited Smart App Banner plugin <= 1.1.3 versions.	5.9	More Details
CVE-2023-39924	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Mitchell Bennis Simple File List plugin <= 6.1.9 versions.	5.9	More Details
CVE-2023-32116	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in TotalPress.Org Custom post types, Custom Fields & more plugin <= 4.0.12 versions.	5.9	More Details
CVE-2023-46088	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Mammothology WP Full Stripe Free plugin <= 1.6.1 versions.	5.9	More Details
CVE-2023-46752	An issue was discovered in FRRouting FRR through 9.0.1. It mishandles malformed MP_REACH_NLRI data, leading to a crash.	5.9	More Details
CVE-2023-31580	light-oauth2 before version 2.1.27 obtains the public key without any verification. This could allow attackers to authenticate to the application with a crafted JWT token.	5.9	More Details
CVE-2023-45767	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Wokamoto Simple Tweet plugin <= 1.4.0.2 versions.	5.9	More Details
CVE-2015-2968	LINE@ for Android version 1.0.0 and LINE@ for iOS version 1.0.0 are vulnerable to MITM (man-in-the-middle) attack since the application allows non-SSL/TLS communications. As a result, any API may be invoked from a script injected by a MITM (man-in-the-middle) attacker.	5.9	More Details
CVE-2023-46093	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in LionScripts.Com Webmaster Tools plugin <= 2.0 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46753	An issue was discovered in FRRouting FRR through 9.0.1. A crash can occur for a crafted BGP UPDATE message without mandatory attributes, e.g., one with only an unknown transit attribute.	5.9	More Details
CVE-2023-45634	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Biztechc Copy or Move Comments plugin <= 5.0.4 versions.	5.8	More Details
CVE-2023-46237	FOG is a free open-source cloning/imaging/rescue suite/inventory management system. Prior to version 1.5.10, an endpoint intended to offer limited enumeration abilities to authenticated users was accessible to unauthenticated users. This enabled unauthenticated users to discover files and their respective paths that were visible to the Apache user group. Version 1.5.10 contains a patch for this issue.	5.8	More Details
CVE-2021-25736	Kube-proxy on Windows can unintentionally forward traffic to local processes listening on the same port (“spec.ports[*].port”) as a LoadBalancer Service when the LoadBalancer controller does not set the “status.loadBalancer.ingress[].ip” field. Clusters where the LoadBalancer controller sets the “status.loadBalancer.ingress[].ip” field are unaffected.	5.8	More Details
CVE-2023-46194	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Eric Teubert Archivist – Custom Archive Templates plugin <= 1.7.5 versions.	5.8	More Details
CVE-2023-27256	Missing authentication in the GetLogFiles method in IDAttend’s IDWeb application 3.1.052 and earlier allows retrieval of sensitive log files by unauthenticated attackers.	5.8	More Details
CVE-2023-43509	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to send notifications to computers that are running ClearPass OnGuard. These notifications can then be used to phish users or trick them into downloading malicious software.	5.8	More Details
CVE-2023-46074	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Borbis Media FreshMail For WordPress plugin <= 2.3.2 versions.	5.8	More Details
CVE-2023-5866	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute in GitHub repository thorsten/phpmyfaq prior to 3.2.1.	5.7	More Details
CVE-2023-43798	BigBlueButton is an open-source virtual classroom. BigBlueButton prior to versions 2.6.12 and 2.7.0-rc.1 is vulnerable to Server-Side Request Forgery (SSRF). This issue is a bypass of CVE-2023-33176. A patch in versions 2.6.12 and 2.7.0-rc.1 disabled follow redirect at `httpclient.execute` since the software no longer has to follow it when using `finalUrl`. There are no known workarounds. We recommend upgrading to a patched version of BigBlueButton.	5.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21301	In ActivityManagerService, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21325	In Settings, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21323	In Activity Manager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21321	In Package Manager, there is a possible cross-user settings disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21320	In Device Policy, there is a possible way to verify if a particular admin app is registered on the device due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21319	In UsageStatsService, there is a possible way to read installed 3rd party apps due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21318	In Content, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21317	In ContentService, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21316	In Content, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-31794	MuPDF v1.21.1 was discovered to contain an infinite recursion in the component pdf_mark_list_push. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted PDF file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21354	In Package Manager Service, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21382	In Content Resolver, there is a possible method to access metadata about existing content providers on the device due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21312	In IntentResolver, there is a possible cross-user media read due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21311	In Settings, there is a possible way to control private DNS settings from a secondary user due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21309	In libcore, 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.	5.5	More Details
CVE-2023-21308	In Composer, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-40139	In FillUi of FillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21306	In ContentService, there is a possible way to read installed sync content providers due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21305	In Content, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21304	In Content Service, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21303	In Content, here is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21383	In Settings, there is a possible way for the user to unintentionally send extra data due to an unclear prompt. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.	5.5	More Details
CVE-2023-21326	In Package Manager Service, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21369	In Usage Access, there is a possible way to display a Settings usage access restriction toggle screen due to a permissions bypass. This could lead to local denial of service with no additional execution privileges needed. User interaction is needed for exploitation.	5.5	More Details
CVE-2023-21327	In Permission Manager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-5785	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3. It has been classified as critical. This affects an unknown part of the file /protocol/firewall/addaddress_interpret.php. The manipulation of the argument messagecontent leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-243591. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-21352	In NFA, 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.	5.5	More Details
CVE-2023-5784	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3 and classified as critical. Affected by this issue is some unknown functionality of the file /protocol/firewall/uploadfirewall.php. The manipulation of the argument messagecontent leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-243590 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-21344	In Job Scheduler, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21385	In Whitechapel, there is a possible out of bounds read due to memory corruption. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-5782	A vulnerability, which was classified as critical, was found in Tongda OA 2017 up to 11.10. Affected is an unknown function of the file /manage/delete_query.php of the component General News. The manipulation of the argument NEWS_ID leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-243588. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-21340	In Telecomm, there is a possible way to get the call state due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-40133	In multiple locations of DialogFillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21338	In Input Method, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21350	In Media Projection, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21336	In Input Method, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21335	In Settings, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21334	In App Ops Service, there is a possible disclosure of information about installed packages due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21333	In Text Services, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21332	In Text Services, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21331	In InputMethod, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21330	In Overlay Manager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21329	In Activity Manager, there is a possible way to determine whether an app is installed due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21384	In Package Manager, there is a possible possible permissions bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21302	In Package Manager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-40123	In updateActionViews of PipMenuView.java, there is a possible bypass of a multi user security boundary due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21300	In PackageManager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-41254	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to access sensitive user data.	5.5	More Details
CVE-2023-40444	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.1. An app may be able to access user-sensitive data.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21376	In Telephony, there is a possible way to retrieve the ICCID due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21299	In Package Manager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-45897	exfatprogs before 1.2.2 allows out-of-bounds memory access, such as in read_file_dentry_set.	5.5	More Details
CVE-2023-40449	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to cause a denial-of-service.	5.5	More Details
CVE-2023-40121	In appendEscapedSQLString of DatabaseUtils.java, there is a possible SQL injection due to unsafe deserialization. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-41072	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. An app may be able to access sensitive user data.	5.5	More Details
CVE-2023-41077	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.6.1. An app may be able to access protected user data.	5.5	More Details
CVE-2023-42854	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. An app may be able to cause a denial-of-service to Endpoint Security clients.	5.5	More Details
CVE-2023-21362	In Usage, there is a possible permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21364	In ContactsProvider, there is a possible crash loop due to resource exhaustion. This could lead to local persistent denial of service in the Phone app with User execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21365	In Contacts, there is a possible crash loop due to resource exhaustion. This could lead to local denial of service in the Phone app with User execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21366	In Scudo, there is a possible way for an attacker to predict heap allocation patterns due to insecure implementation/design. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-5827	A vulnerability was found in Shanghai CTI Navigation CTI Monitoring and Early Warning System 2.2. It has been classified as critical. This affects an unknown part of the file /Web/SysManage/UserEdit.aspx. The manipulation of the argument ID leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-243717 was assigned to this vulnerability.	5.5	More Details
CVE-2023-5826	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/list_onlineuser.php. The manipulation of the argument SessionId leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-243716. NOTE: We tried to contact the vendor early about the disclosure but the official mail address was not working properly.	5.5	More Details
CVE-2023-40101	In collapse of canonicalize_md.c, 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.	5.5	More Details
CVE-2023-21368	In Audio, there is a possible out of bounds read due to missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-40421	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. An app may be able to access sensitive user data.	5.5	More Details
CVE-2005-10002	A vulnerability, which was classified as critical, was found in almosteffortless secure-files Plugin up to 1.1 on WordPress. Affected is the function sf_downloads of the file secure-files.php. The manipulation of the argument downloadfile leads to path traversal. Upgrading to version 1.2 is able to address this issue. The name of the patch is cab025e5fc2bcdad8032d833ebc38e6bd2a13c92. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-243804.	5.5	More Details
CVE-2023-5745	The Reusable Text Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'text-blocks' shortcode in versions up to, and including, 1.5.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with author-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.5	More Details
CVE-2023-46407	FFmpeg prior to commit bf814 was discovered to contain an out of bounds read via the dist->alphabet_size variable in the read_vlc_prefix() function.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21296	In Permission, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	5.5	More Details
CVE-2023-21295	In SliceManagerService, there is a possible way to check if a content provider is installed due to a missing null check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21294	In Slice, there is a possible disclosure of installed packages due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21293	In PackageManagerNative, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2022-20264	In Usage Stats Service, there is a possible way to determine whether an app is installed, without query permissions due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21367	In Scudo, there is a possible way to exploit certain heap OOB read/write issues due to an insecure implementation/design. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21394	In registerPhoneAccount of TelecomServiceImpl.java, there is a possible way to reveal images from another user due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-46316	In buc Traceroute 2.0.12 through 2.1.2 before 2.1.3, the wrapper scripts do not properly parse command lines.	5.5	More Details
CVE-2023-42842	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.1. An app may be able to access sensitive user data.	5.5	More Details
CVE-2023-44323	Adobe Acrobat for Edge version 118.0.2088.46 (and earlier) is affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42850	The issue was addressed with improved permissions logic. This issue is fixed in macOS Sonoma 14.1. An app may be able to access sensitive user data.	5.5	More Details
CVE-2023-5752	When installing a package from a Mercurial VCS URL (ie "pip install hg+...") with pip prior to v23.3, the specified Mercurial revision could be used to inject arbitrary configuration options to the "hg clone" call (ie "--config"). Controlling the Mercurial configuration can modify how and which repository is installed. This vulnerability does not affect users who aren't installing from Mercurial.	5.5	More Details
CVE-2023-40413	The issue was addressed with improved handling of caches. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to read sensitive location information.	5.5	More Details
CVE-2023-21377	In SELinux Policy, there is a possible restriction bypass due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-5873	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 11.1.0.	5.4	More Details
CVE-2023-5867	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.2.2.	5.4	More Details
CVE-2023-5458	The CITS Support svg, webp Media and TTF,OTF File Upload WordPress plugin before 3.0 does not sanitise uploaded SVG files, which could allow users with a role as low as Author to upload a malicious SVG containing XSS payloads.	5.4	More Details
CVE-2023-46040	Cross Site Scripting vulnerability in GetSimpleCMS v.3.4.0a allows a remote attacker to execute arbitrary code via the a crafted payload to the components.php function.	5.4	More Details
CVE-2023-5237	The Memberlite Shortcodes WordPress plugin before 1.3.9 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admin.	5.4	More Details
CVE-2023-4823	The WP Meta and Date Remover WordPress plugin before 2.2.0 provides an AJAX endpoint for configuring the plugin settings. This endpoint has no capability checks and does not sanitize the user input, which is then later output unescaped. Allowing any authenticated users, such as subscriber change them and perform Stored Cross-Site Scripting.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5114	The idbbee plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'idbbee' shortcode in versions up to, and including, 1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2023-46235	FOG is a free open-source cloning/imaging/rescue suite/inventory management system. Prior to version 1.5.10.15, due to a lack of request sanitization in the logs, a malicious request containing XSS would be stored in a log file. When an administrator of the FOG server logged in and viewed the logs, they would be parsed as HTML and displayed accordingly. Version 1.5.10.15 contains a patch. As a workaround, view logs from an external text editor rather than the dashboard.	5.4	More Details
CVE-2022-39172	A stored XSS in the process overview (bersicht zugewiesener Vorgaenge) in mbsupport openVIVA c2 20220101 allows a remote, authenticated, low-privileged attacker to execute arbitrary code in the victim's browser via name field of a process.	5.4	More Details
CVE-2023-46451	Best Courier Management System v1.0 is vulnerable to Cross Site Scripting (XSS) in the change username field.	5.4	More Details
CVE-2023-46378	Stored Cross Site Scripting (XSS) vulnerability in MiniCMS 1.1.1 allows attackers to run arbitrary code via crafted string appended to /mc-admin/conf.php.	5.4	More Details
CVE-2023-44769	A Cross-Site Scripting (XSS) vulnerability in Zenario CMS v.9.4.59197 allows a local attacker to execute arbitrary code via a crafted script to the Spare aliases from Alias.	5.4	More Details
CVE-2023-46396	Audimex 15.0.0 is vulnerable to Cross Site Scripting (XSS) in /audimex/cgi-bin/wal.fcgi via company parameter search filters.	5.4	More Details
CVE-2023-46854	Proxmox proxmox-widget-toolkit before 4.0.9, as used in multiple Proxmox products, allows XSS via the edit notes feature.	5.4	More Details
CVE-2023-46858	Moodle 4.3 allows /grade/report/grader/index.php?searchvalue= reflected XSS when logged in as a teacher. NOTE: the Moodle Security FAQ link states "Some forms of rich content [are] used by teachers to enhance their courses ... admins and teachers can post XSS-capable content, but students can not."	5.4	More Details
CVE-2023-46150	Cross-Site Request Forgery (CSRF) vulnerability in WP Military WP Radio plugin <= 3.1.9 versions.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4393	HTML and SMTP injections on the registration page of LiquidFiles versions 3.7.13 and below, allow an attacker to perform more advanced phishing attacks against an organization.	5.4	More Details
CVE-2023-46450	Sourcecodester Free and Open Source inventory management system 1.0 is vulnerable to Cross Site Scripting (XSS) via the Add supplier function.	5.4	More Details
CVE-2023-45746	Cross-site scripting vulnerability in Movable Type series allows a remote authenticated attacker to inject an arbitrary script. Affected products/versions are as follows: Movable Type 7 r.5405 and earlier (Movable Type 7 Series), Movable Type Advanced 7 r.5405 and earlier (Movable Type 7 Series), Movable Type Premium 1.58 and earlier, Movable Type Premium Advanced 1.58 and earlier, Movable Type Cloud Edition (Version 7) r.5405 and earlier, and Movable Type Premium Cloud Edition 1.58 and earlier.	5.4	More Details
CVE-2023-43360	Cross Site Scripting vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted script to the Top Directory parameter in the File Picker Menu component.	5.4	More Details
CVE-2023-46467	Cross Site Scripting vulnerability in juzawebCMS v.3.4 and before allows a remote attacker to execute arbitrary code via a crafted payload to the username parameter of the registration page.	5.4	More Details
CVE-2022-34833	An issue was discovered in VERMEG AgileReporter 21.3. An admin can enter an XSS payload in the Analysis component.	5.4	More Details
CVE-2023-46198	Cross-Site Request Forgery (CSRF) vulnerability in Scientech It Solution Appointment Calendar plugin <= 2.9.6 versions.	5.4	More Details
CVE-2023-46650	Jenkins GitHub Plugin 1.37.3 and earlier does not escape the GitHub project URL on the build page when showing changes, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2023-46394	A stored cross-site scripting (XSS) vulnerability in /home/user/edit_submit of gougucms v4.08.18 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the headimgurl parameter.	5.4	More Details
CVE-2023-5251	The Grid Plus plugin for WordPress is vulnerable to unauthorized modification of data and loss of data due to a missing capability check on the 'grid_plus_save_layout_callback' and 'grid_plus_delete_callback' functions in versions up to, and including, 1.3.2. This makes it possible for authenticated attackers with subscriber privileges or above, to add, update or delete grid layout.	5.4	More Details
CVE-2023-46504	Cross Site Scripting (XSS) vulnerability in PwnCYN YXBOOKCMS v.1.0.2 allows a physically proximate attacker to execute arbitrary code via the library name function in the general settings component.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46659	Jenkins Edgewall Trac Plugin 1.13 and earlier does not escape the Trac website URL on the build page, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2023-42845	An authentication issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. Photos in the Hidden Photos Album may be viewed without authentication.	5.3	More Details
CVE-2023-42846	This issue was addressed by removing the vulnerable code. This issue is fixed in watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, tvOS 17.1, iOS 17.1 and iPadOS 17.1. A device may be passively tracked by its Wi-Fi MAC address.	5.3	More Details
CVE-2023-46656	Jenkins Multibranch Scan Webhook Trigger Plugin 1.0.9 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token are equal, potentially allowing attackers to use statistical methods to obtain a valid webhook token.	5.3	More Details
CVE-2023-46657	Jenkins Gogs Plugin 1.0.15 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token are equal, potentially allowing attackers to use statistical methods to obtain a valid webhook token.	5.3	More Details
CVE-2023-46658	Jenkins MSTeams Webhook Trigger Plugin 0.1.1 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token are equal, potentially allowing attackers to use statistical methods to obtain a valid webhook token.	5.3	More Details
CVE-2023-46137	Twisted is an event-based framework for internet applications. Prior to version 23.10.0rc1, when sending multiple HTTP requests in one TCP packet, twisted.web will process the requests asynchronously without guaranteeing the response order. If one of the endpoints is controlled by an attacker, the attacker can delay the response on purpose to manipulate the response of the second request when a victim launched two requests using HTTP pipeline. Version 23.10.0rc1 contains a patch for this issue.	5.3	More Details
CVE-2023-46135	rs-stellar-strkey is a Rust lib for encode/decode of Stellar Strkeys. A panic vulnerability occurs when a specially crafted payload is used.`inner_payload_len` should not above 64. This vulnerability has been patched in version 0.0.8.	5.3	More Details
CVE-2023-46666	An issue was discovered when using Document Level Security and the SPO "Limited Access" functionality in Elastic Sharepoint Online Python Connector. If a user is assigned limited access permissions to an item on a Sharepoint site then that user would have read permissions to all content on the Sharepoint site through Elasticsearch.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46123	jumpserver is an open source bastion machine, professional operation and maintenance security audit system that complies with 4A specifications. A flaw in the Core API allows attackers to bypass password brute-force protections by spoofing arbitrary IP addresses. By exploiting this vulnerability, attackers can effectively make unlimited password attempts by altering their apparent IP address for each request. This vulnerability has been patched in version 3.8.0.	5.3	More Details
CVE-2023-46660	Jenkins Zanata Plugin 0.6 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token hashes are equal, potentially allowing attackers to use statistical methods to obtain a valid webhook token.	5.3	More Details
CVE-2023-5349	A memory leak flaw was found in ruby-magick, an interface between Ruby and ImageMagick. This issue can lead to a denial of service (DOS) by memory exhaustion.	5.3	More Details
CVE-2023-4693	An out-of-bounds read flaw was found on grub2's NTFS filesystem driver. This issue may allow a physically present attacker to present a specially crafted NTFS file system image to read arbitrary memory locations. A successful attack allows sensitive data cached in memory or EFI variable values to be leaked, presenting a high Confidentiality risk.	5.3	More Details
CVE-2023-5722	Using iterative requests an attacker was able to learn the size of an opaque response, as well as the contents of a server-supplied Vary header. This vulnerability affects Firefox < 119.	5.3	More Details
CVE-2023-27261	Missing authentication in the DeleteAssignments method in IDAttend's IDWeb application 3.1.052 and earlier allows deletion of data by unauthenticated attackers.	5.3	More Details
CVE-2023-5723	An attacker with temporary script access to a site could have set a cookie containing invalid characters using `document.cookie` that could have led to unknown errors. This vulnerability affects Firefox < 119.	5.3	More Details
CVE-2023-46232	era-compiler-vyper is the EraVM Vyper compiler for zkSync Era, a layer 2 rollup that uses zero-knowledge proofs to scale Ethereum. Prior to era-compiler-vype version 1.3.10, a bug prevented the initialization of the first immutable variable for Vyper contracts meeting certain criteria. The problem arises when there is a String or Array with more 256-bit words allocated than initialized. It results in the second word's index unset, that is effectively set to 0, so the first immutable value with the actual 0 index is overwritten in the ImmutableSimulator. Version 1.3.10 fixes this issue by setting all indexes in advance. The problem will go away, but it will get more expensive if the user allocates a lot of uninitialized space, e.g. `String[4096]`. Upgrading and redeploying affected contracts is the only way of working around the issue.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5786	A vulnerability was found in GeoServer GeoWebCache up to 1.15.1. It has been declared as problematic. This vulnerability affects unknown code of the file /geoserver/gwc/rest.html. The manipulation leads to direct request. 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-243592.	5.3	More Details
CVE-2023-46864	Peppermint Ticket Management through 0.2.4 allows remote attackers to read arbitrary files via a /api/v1/ticket/1/file/download?filepath=../ POST request.	5.3	More Details
CVE-2023-39695	Insufficient session expiration in Elenos ETG150 FM Transmitter v3.12 allows attackers to arbitrarily change transmitter configuration and data after logging out.	5.3	More Details
CVE-2023-26579	Missing authentication in the DeleteStaff method in IDAttend's IDWeb application 3.1.013 allows deletion of staff information by unauthenticated attackers.	5.3	More Details
CVE-2023-42803	BigBlueButton is an open-source virtual classroom. BigBlueButton prior to version 2.6.0-beta.2 is vulnerable to unrestricted file upload, where the insertDocument API call does not validate the given file extension before saving the file, and does not remove it in case of validation failures. BigBlueButton 2.6.0-beta.2 contains a patch. There are no known workarounds.	5.3	More Details
CVE-2023-41721	Instances of UniFi Network Application that (i) are run on a UniFi Gateway Console, and (ii) are versions 7.5.176. and earlier, implement device adoption with improper access control logic, creating a risk of access to device configuration information by a malicious actor with preexisting access to the network. Affected Products: UDM UDM-PRO UDM-SE UDR UDW Mitigation: Update UniFi Network to Version 7.5.187 or later.	5.3	More Details
CVE-2023-31416	Secret token configuration is never applied when using ECK <2.8 with APM Server >=8.0. This could lead to anonymous requests to an APM Server being accepted and the data ingested into this APM deployment.	5.3	More Details
CVE-2023-46754	The admin panel for Obl.ong before 1.1.2 allows authorization bypass because the email OTP feature accepts arbitrary numerical values.	5.3	More Details
CVE-2023-43796	Synapse is an open-source Matrix homeserver Prior to versions 1.95.1 and 1.96.0rc1, cached device information of remote users can be queried from Synapse. This can be used to enumerate the remote users known to a homeserver. System administrators are encouraged to upgrade to Synapse 1.95.1 or 1.96.0rc1 to receive a patch. As a workaround, the `federation_domain_whitelist` can be used to limit federation traffic with a homeserver.	5.3	More Details
CVE-2023-37831	An issue discovered in Elenos ETG150 FM transmitter v3.12 allows attackers to enumerate user accounts based on server responses when credentials are submitted.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40408	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. Hide My Email may be deactivated unexpectedly.	5.3	More Details
CVE-2023-46250	pypdf is a free and open-source pure-python PDF library. An attacker who uses a vulnerability present in versions 3.7.0 through 3.16.4 can craft a PDF which leads to an infinite loop. This infinite loop blocks the current process and can utilize a single core of the CPU by 100%. It does not affect memory usage. That is, for example, the case when the pypdf-user manipulates an incoming malicious PDF e.g. by merging it with another PDF or by adding annotations. The issue was fixed in version 3.17.0. As a workaround, apply the patch manually by modifying `pypdf/generic/_data_structures.py`.	5.1	More Details
CVE-2023-21307	In Bluetooth, there is a possible way for a paired Bluetooth device to access a long term identifier for an Android device due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.	5.0	More Details
CVE-2023-46139	KernelSU is a Kernel based root solution for Android. Starting in version 0.6.1 and prior to version 0.7.0, if a KernelSU installed device is infected with a malware whose app signing block specially constructed, it can take over root privileges on the device. The vulnerable verification logic actually obtains the signature of the last block with an id of `0x7109871a`, while the verification logic during Android installation is to obtain the first one. In addition to the actual signature upgrade that has been fixed (KSU thought it was V2 but was actually V3), there is also the problem of actual signature downgrading (KSU thought it was V2 but was actually V1). Find a condition in the signature verification logic that will cause the signature not to be found error, and KernelSU does not implement the same conditions, so KSU thinks there is a V2 signature, but the APK signature verification actually uses the V1 signature. This issue is fixed in version 0.7.0. As workarounds, keep the KernelSU manager installed and avoid installing unknown apps.	5.0	More Details
CVE-2023-5126	The Delete Me plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'plugin_delete_me' shortcode in versions up to, and including, 3.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The shortcode is not displayed to administrators, so it cannot be used against administrator users.	4.9	More Details
CVE-2023-38328	An issue was discovered in eGroupWare 17.1.20190111. An Improper Password Storage vulnerability affects the setup panel of under setup/manageheader.php, which allows authenticated remote attackers with administrator credentials to read a cleartext database password.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46120	The RabbitMQ Java client library allows Java and JVM-based applications to connect to and interact with RabbitMQ nodes. `maxBodyLebgth` was not used when receiving Message objects. Attackers could send a very large Message causing a memory overflow and triggering an OOM Error. Users of RabbitMQ may suffer from DoS attacks from RabbitMQ Java client which will ultimately exhaust the memory of the consumer. This vulnerability was patched in version 5.18.0.	4.9	More Details
CVE-2023-43648	baserCMS is a website development framework. Prior to version 4.8.0, there is a Directory Traversal Vulnerability in the form submission data management feature of baserCMS. Version 4.8.0 contains a patch for this issue.	4.9	More Details
CVE-2023-46158	IBM WebSphere Application Server Liberty 23.0.0.9 through 23.0.0.10 could provide weaker than expected security due to improper resource expiration handling. IBM X-Force ID: 268775.	4.9	More Details
CVE-2023-46118	RabbitMQ is a multi-protocol messaging and streaming broker. HTTP API did not enforce an HTTP request body limit, making it vulnerable for denial of service (DoS) attacks with very large messages. An authenticated user with sufficient credentials can publish a very large messages over the HTTP API and cause target node to be terminated by an "out-of-memory killer"-like mechanism. This vulnerability has been patched in versions 3.11.24 and 3.12.7.	4.9	More Details
CVE-2023-40686	Management Central as part of IBM i 7.2, 7.3, 7.4, and 7.5 Navigator contains a local privilege escalation vulnerability. A malicious actor with command line access to the operating system can exploit this vulnerability to elevate privileges to gain component access to the operating system. IBM X-Force ID: 264114.	4.9	More Details
CVE-2023-42031	IBM TXSeries for Multiplatforms, 8.1, 8.2, and 9.1, CICS TX Standard CICS TX Advanced 10.1 and 11.1 could allow a privileged user to cause a denial of service due to uncontrolled resource consumption. IBM X-Force ID: 266016.	4.9	More Details
CVE-2023-29973	Pfsense CE version 2.6.0 is vulnerable to No rate limit which can lead to an attacker creating multiple malicious users in firewall.	4.9	More Details
CVE-2023-5861	Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 2.0.	4.8	More Details
CVE-2022-34834	An issue was discovered in VERMEG AgileReporter 21.3. Attackers can gain privileges via an XSS payload in an Add Comment action to the Activity log.	4.8	More Details
CVE-2023-5864	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.2.1.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5243	The Login Screen Manager WordPress plugin through 3.5.2 does not sanitize and escape some of its settings, which could allow high-privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2023-5842	Cross-site Scripting (XSS) - Stored in GitHub repository dolibarr/dolibarr prior to 16.0.5.	4.8	More Details
CVE-2023-44767	A File upload vulnerability in RiteCMS 3.0 allows a local attacker to upload a SVG file with XSS content.	4.8	More Details
CVE-2023-4390	The Popup box WordPress plugin before 3.7.2 does not sanitize and escape some Popup fields, which could allow high-privilege users such as an administrator to inject arbitrary web scripts even when the unfiltered_html capability is disallowed (for example in a multisite setup).	4.8	More Details
CVE-2023-5229	The E2Pdf WordPress plugin before 1.20.20 does not sanitize and escape some of its settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2023-45671	Frigate is an open source network video recorder. Prior to version 0.13.0 Beta 3, there is a reflected cross-site scripting vulnerability in any API endpoints reliant on the `/<camera_name>` base path as values provided for the path are not sanitized. Exploiting this vulnerability requires the attacker to both know very specific information about a user's Frigate server and requires an authenticated user to be tricked into clicking a specially crafted link to their Frigate instance. This vulnerability could exploited by an attacker under the following circumstances: Frigate publicly exposed to the internet (even with authentication); attacker knows the address of a user's Frigate instance; attacker crafts a specialized page which links to the user's Frigate instance; attacker finds a way to get an authenticated user to visit their specialized page and click the button/link. As the reflected values included in the URL are not sanitized or escaped, this permits execution arbitrary Javascript payloads. Version 0.13.0 Beta 3 contains a patch for this issue.	4.7	More Details
CVE-2023-43510	A vulnerability in the ClearPass Policy Manager web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as a non-privileged user on the underlying operating system leading to partial system compromise.	4.7	More Details
CVE-2023-46862	An issue was discovered in the Linux kernel through 6.5.9. During a race with SQ thread exit, an io_uring/fdinfo.c io_uring_show_fdinfo NULL pointer dereference can occur.	4.7	More Details
CVE-2023-43649	baserCMS is a website development framework. Prior to version 4.8.0, there is a cross site request forgery vulnerability in the content preview feature of baserCMS. Version 4.8.0 contains a patch for this issue.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5812	A vulnerability has been found in flusity CMS and classified as critical. Affected by this vulnerability is the function handleFileUpload of the file core/tools/upload.php. The manipulation of the argument uploaded_file leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The associated identifier of this vulnerability is VDB-243643.	4.7	More Details
CVE-2023-5380	A use-after-free flaw was found in the xorg-x11-server. An X server crash may occur in a very specific and legacy configuration (a multi-screen setup with multiple protocol screens, also known as Zaphod mode) if the pointer is warped from within a window on one screen to the root window of the other screen and if the original window is destroyed followed by another window being destroyed.	4.7	More Details
CVE-2023-41982	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data.	4.6	More Details
CVE-2023-41997	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data.	4.6	More Details
CVE-2023-46668	If Elastic Endpoint (v7.9.0 - v8.10.3) is configured to use a non-default option in which the logging level is explicitly set to debug, and when Elastic Agent is simultaneously configured to collect and send those logs to Elasticsearch, then Elastic Agent API keys can be viewed in Elasticsearch in plaintext. These API keys could be used to write arbitrary data and read Elastic Endpoint user artifacts.	4.6	More Details
CVE-2023-5139	Potential buffer overflow vulnerability at the following location in the Zephyr STM32 Crypto driver	4.4	More Details
CVE-2023-40425	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Monterey 12.7.1. An app with root privileges may be able to access private information.	4.4	More Details
CVE-2023-46256	PX4-Autopilot provides PX4 flight control solution for drones. In versions 1.14.0-rc1 and prior, PX4-Autopilot has a heap buffer overflow vulnerability in the parser function due to the absence of `parserbuf_index` value checking. A malfunction of the sensor device can cause a heap buffer overflow with leading unexpected drone behavior. Malicious applications can exploit the vulnerability even if device sensor malfunction does not occur. Up to the maximum value of an `unsigned int`, bytes sized data can be written to the heap memory area. As of time of publication, no fixed version is available.	4.4	More Details
CVE-2022-3698	A denial of service vulnerability was reported in the Lenovo HardwareScanPlugin versions prior to 1.3.1.2 and Lenovo Diagnostics versions prior to 4.45 that could allow a local user with administrative access to trigger a system crash.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0353	A denial of service vulnerability was reported in the Lenovo HardwareScanPlugin versions prior to 1.3.1.2 and Lenovo Diagnostics versions prior to 4.45 that could allow a local user with administrative access to trigger a system crash.	4.4	More Details
CVE-2023-21297	In SEPolicy, there is a possible way to access the factory MAC address due to a permissions bypass. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	4.4	More Details
CVE-2023-21359	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server with System execution privileges needed. User interaction is not needed for exploitation.	4.4	More Details
CVE-2023-21357	In NFC, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	4.4	More Details
CVE-2023-21314	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	4.4	More Details
CVE-2023-21379	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server with System execution privileges needed. User interaction is not needed for exploitation.	4.4	More Details
CVE-2023-21387	In User Backup Manager, there is a possible way to leak a token to bypass user confirmation for backup due to log information disclosure. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	4.4	More Details
CVE-2023-46151	Cross-Site Request Forgery (CSRF) vulnerability in AWESOME TOGI Product Category Tree plugin <= 2.5 versions.	4.3	More Details
CVE-2023-46189	Cross-Site Request Forgery (CSRF) vulnerability in Simple Calendar – Google Calendar Plugin <= 3.2.5 versions.	4.3	More Details
CVE-2023-5721	It was possible for certain browser prompts and dialogs to be activated or dismissed unintentionally by the user due to an insufficient activation-delay. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	4.3	More Details
CVE-2023-46190	Cross-Site Request Forgery (CSRF) vulnerability in Novo-media Novo-Map : your WP posts on custom google maps plugin <= 1.1.2 versions.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5519	The EventPrime WordPress plugin before 3.2.0 does not have CSRF checks when creating bookings, which could allow attackers to make logged in users create unwanted bookings via CSRF attacks.	4.3	More Details
CVE-2023-46191	Cross-Site Request Forgery (CSRF) vulnerability in Niels van Renselaar Open Graph Metabox plugin <= 1.4.4 versions.	4.3	More Details
CVE-2023-5821	The Thumbnail carousel slider plugin for WordPress is vulnerable to Cross-Site Request Forgery in version 1.0. This is due to missing nonce validation on the deleteselected function. This makes it possible for unauthenticated attackers to delete sliders in bulk via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-46193	Cross-Site Request Forgery (CSRF) vulnerability in Internet Marketing Ninjas Internal Link Building plugin <= 1.2.3 versions.	4.3	More Details
CVE-2023-46652	A missing permission check in Jenkins lambdatest-automation Plugin 1.20.9 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of LAMBDATEST credentials stored in Jenkins.	4.3	More Details
CVE-2022-34887	Standard users can directly operate and set printer configuration information , such as IP, in some Lenovo Printers without having to authenticate with the administrator password.	4.3	More Details
CVE-2023-46204	Cross-Site Request Forgery (CSRF) vulnerability in Muller Digital Inc. Duplicate Theme plugin <= 0.1.6 versions.	4.3	More Details
CVE-2023-5725	A malicious installed WebExtension could open arbitrary URLs, which under the right circumstance could be leveraged to collect sensitive user data. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	4.3	More Details
CVE-2023-5726	A website could have obscured the full screen notification by using the file open dialog. This could have led to user confusion and possible spoofing attacks. *Note: This issue only affected macOS operating systems. Other operating systems are unaffected.* This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	4.3	More Details
CVE-2023-5729	A malicious web site can enter fullscreen mode while simultaneously triggering a WebAuthn prompt. This could have obscured the fullscreen notification and could have been leveraged in a spoofing attack. This vulnerability affects Firefox < 119.	4.3	More Details
CVE-2023-42438	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.1. Visiting a malicious website may lead to user interface spoofing.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4836	The WordPress File Sharing Plugin WordPress plugin before 2.0.5 does not check authorization before displaying files and folders, allowing users to gain access to those filed by manipulating IDs which can easily be brute forced	4.3	More Details
CVE-2023-46152	Cross-Site Request Forgery (CSRF) vulnerability in realmag777 WOLF – WordPress Posts Bulk Editor and Manager Professional plugin <= 1.0.7.1 versions.	4.3	More Details
CVE-2023-5802	Cross-Site Request Forgery (CSRF) vulnerability in Mihai Iova WordPress Knowledge base & Documentation Plugin – WP Knowledgebase plugin <= 1.3.4 versions.	4.3	More Details
CVE-2023-4251	The EventPrime WordPress plugin before 3.2.0 does not have CSRF checks when creating bookings, which could allow attackers to make logged in users create unwanted bookings via CSRF attacks.	4.3	More Details
CVE-2023-34056	vCenter Server contains a partial information disclosure vulnerability. A malicious actor with non-administrative privileges to vCenter Server may leverage this issue to access unauthorized data.	4.3	More Details
CVE-2023-46202	Cross-Site Request Forgery (CSRF) vulnerability in Jeff Sherk Auto Login New User After Registration plugin <= 1.9.6 versions.	4.3	More Details
CVE-2023-41977	The issue was addressed with improved handling of caches. This issue is fixed in macOS Sonoma 14.1, iOS 16.7.2 and iPadOS 16.7.2. Visiting a malicious website may reveal browsing history.	4.3	More Details
CVE-2023-41975	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. A website may be able to access the microphone without the microphone use indicator being shown.	4.3	More Details
CVE-2023-46255	SpiceDB is an open source, Google Zanzibar-inspired database for creating and managing security-critical application permissions. Prior to version 1.27.0-rc1, when the provided datastore URI is malformed (e.g. by having a password which contains `:`) the full URI (including the provided password) is printed, so that the password is shown in the logs. Version 1.27.0-rc1 patches this issue.	4.2	More Details
CVE-2023-4608	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected.	4.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31417	Elasticsearch generally filters out sensitive information and credentials before logging to the audit log. It was found that this filtering was not applied when requests to Elasticsearch use certain deprecated URIs for APIs. The impact of this flaw is that sensitive information such as passwords and tokens might be printed in cleartext in Elasticsearch audit logs. Note that audit logging is disabled by default and needs to be explicitly enabled and even when audit logging is enabled, request bodies that could contain sensitive information are not printed to the audit log unless explicitly configured.	4.1	More Details
CVE-2023-46246	Vim is an improved version of the good old UNIX editor Vi. Heap-use-after-free in memory allocated in the function `ga_grow_inner` in in the file `src/alloc.c` at line 748, which is freed in the file `src/ex_docmd.c` in the function `do_cmdline` at line 1010 and then used again in `src/cmdhist.c` at line 759. When using the `:history` command, it's possible that the provided argument overflows the accepted value. Causing an Integer Overflow and potentially later an use-after-free. This vulnerability has been patched in version 9.0.2068.	4.0	More Details
CVE-2023-46126	Fides is an open-source privacy engineering platform for managing the fulfillment of data privacy requests in runtime environments, helping enforce privacy regulations in code. The Fides web application allows users to edit consent and privacy notices such as cookie banners. The vulnerability makes it possible to craft a payload in the privacy policy URL which triggers JavaScript execution when the privacy notice is served by an integrated website. The domain scope of the executed JavaScript is that of the integrated website. Exploitation is limited to Admin UI users with the contributor role or higher. The vulnerability has been patched in Fides version `2.22.1`.	3.9	More Details
CVE-2023-5834	HashiCorp Vagrant's Windows installer targeted a custom location with a non-protected path that could be junctioned, introducing potential for unauthorized file system writes. Fixed in Vagrant 2.4.0.	3.8	More Details
CVE-2023-46138	JumpServer is an open source bastion host and maintenance security audit system that complies with 4A specifications. Prior to version 3.8.0, the default email for initial user admin is `admin[@]mycompany[.]com`, and users reset their passwords by sending an email. Currently, the domain `mycompany.com` has not been registered. However, if it is registered in the future, it may affect the password reset functionality. This issue has been patched in version 3.8.0 by changing the default email domain to `example.com`. Those who cannot upgrade may change the default email domain to `example.com` manually.	3.7	More Details
CVE-2023-5835	A vulnerability classified as problematic was found in hu60t hu60wap6. Affected by this vulnerability is the function markdown of the file src/class/ubbparser.php. The manipulation leads to cross site scripting. The attack can be launched remotely. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The patch is named a1cd9f12d7687243bfcb7ce295665acb83b9174e. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-243775.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5837	A vulnerability classified as problematic was found in AlexanderLivanov FotosCMS2 up to 2.4.3. This vulnerability affects unknown code of the file profile.php of the component Cookie Handler. The manipulation of the argument username leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-243802 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-41891	FlyteAdmin is the control plane for Flyte responsible for managing entities and administering workflow executions. Prior to version 1.1.124, list endpoints on FlyteAdmin have a SQL vulnerability where a malicious user can send a REST request with custom SQL statements as list filters. The attacker needs to have access to the FlyteAdmin installation, typically either behind a VPN or authentication. Version 1.1.124 contains a patch for this issue.	3.5	More Details
CVE-2023-5793	A vulnerability was found in flusity CMS and classified as problematic. This issue affects the function loadCustomBlocCreateForm of the file /core/tools/customblock.php of the component Dashboard. The manipulation of the argument customblock_place leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The patch is named 81252bc764e1de2422e79e36194bba1289e7a0a5. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-243599.	3.5	More Details
CVE-2023-5791	A vulnerability, which was classified as problematic, was found in SourceCodester Sticky Notes App 1.0. This affects an unknown part of the file endpoint/add-note.php. The manipulation of the argument noteTitle/noteContent 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 identifier VDB-243597 was assigned to this vulnerability.	3.5	More Details
CVE-2023-43295	Cross Site Request Forgery vulnerability in Click Studios (SA) Pty Ltd Passwordstate v.Build 9785 and before allows a local attacker to execute arbitrary code via a crafted request.	3.5	More Details
CVE-2023-40138	In FillUi of FillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details
CVE-2023-40136	In setHeader of DialogFillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40137	In multiple functions of DialogFillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details
CVE-2023-21345	In Game Manager Service, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details
CVE-2023-21346	In the Device Idle Controller, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details
CVE-2023-5862	Missing Authorization in GitHub repository hamza417/inure prior to Build95.	3.3	More Details
CVE-2023-21349	In Package Manager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details
CVE-2023-40135	In applyCustomDescription of SaveUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details
CVE-2023-21348	In Window Manager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details
CVE-2023-40134	In isFullScreen of FillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details
CVE-2023-42857	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. An app may be able to access sensitive user data.	3.3	More Details
CVE-2023-40405	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sonoma 14.1. An app may be able to read sensitive location information.	3.3	More Details
CVE-2023-40127	In multiple locations, there is a possible way to access screenshots due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42804	BigBlueButton is an open-source virtual classroom. BigBlueButton prior to version 2.6.0-beta.1 has a path traversal vulnerability that allows an attacker with a valid starting folder path, to traverse and read other files without authentication, assuming the files have certain extensions (txt, swf, svg, png). In version 2.6.0-beta.1, input validation was added on the parameters being passed and dangerous characters are stripped. There are no known workarounds.	3.1	More Details
CVE-2023-37833	Improper access control in Elenos ETG150 FM transmitter v3.12 allows attackers to make arbitrary configuration edits that are only accessed by privileged users.	2.7	More Details
CVE-2023-34085	When an AWS DynamoDB table is used for user attribute storage, it is possible to retrieve the attributes of another user using a maliciously crafted request	2.6	More Details
CVE-2023-5789	A vulnerability classified as problematic has been found in Dragon Path 707GR1 up to 20231022. Affected is an unknown function of the component Ping Diagnostics. The manipulation of the argument Host Address with the input >> <img/src/onerror=alert(1)> leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-243594 is the identifier assigned to this vulnerability.	2.4	More Details
CVE-2023-5811	A vulnerability, which was classified as problematic, was found in flusity CMS. Affected is the function loadPostAddForm of the file core/tools/posts.php. The manipulation of the argument menu_id leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The patch is identified as 6943991c62ed87c7a57989a0cb7077316127def8. It is recommended to apply a patch to fix this issue. VDB-243642 is the identifier assigned to this vulnerability.	2.4	More Details
CVE-2023-5810	A vulnerability, which was classified as problematic, has been found in flusity CMS. This issue affects the function loadPostAddForm of the file core/tools/posts.php. The manipulation of the argument edit_post_id leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The identifier of the patch is 6943991c62ed87c7a57989a0cb7077316127def8. It is recommended to apply a patch to fix this issue. The identifier VDB-243641 was assigned to this vulnerability.	2.4	More Details
CVE-2023-42431	Cross-site Scripting (XSS) vulnerability in BlueSpiceAvatars extension of BlueSpice allows logged in user to inject arbitrary HTML into the profile image dialog on Special:Preferences. This only applies to the genuine user context.	2.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44268	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-41377	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2023. Notes: none.	N/A	More Details
CVE-2023-5306	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-43737	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-44486	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-23767	Rejected reason: This CVE ID has been rejected or withdrawn by GitHub as it was issued in error.	N/A	More Details
CVE-2023-44078	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-2023-44485	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-45804	Rejected reason: User requested a CVE number by mistake	N/A	More Details
CVE-2023-39816	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-2023-39814	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-2023-39815	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-2023-41605	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40943	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-2023-39817	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-48190	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2020-25870	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-2018-11103	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-2023-44002	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-2023-45960	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-43738	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-44162	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-44375	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-44376	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-44377	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4610	Rejected reason: The SRCU code was added in upstream kernel v6.4-rc1 and removed before v6.4. This bug only existed in development kernels. Please see https://lore.kernel.org/all/ZTKVfoQZplpB8rki@casper.infradead.org and https://bugzilla.suse.com/show_bug.cgi?id=1215932 for more information.	N/A	More Details