SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 30 November 2022

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-41875	A remote code execution (RCE) vulnerability in Optica allows unauthenticated attackers to execute arbitrary code via specially crafted JSON payloads. Specially crafted JSON payloads may lead to RCE (remote code execution) on the attacked system running Optica. The vulnerability was patched in v. 0.10.2, where the call to the function `oj.load` was changed to `oj.safe_load`.	10.0	More Details
CVE-2022-41934	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with view rights on commonly accessible documents including the menu macro can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation due to improper escaping of the macro content and parameters of the menu macro. The problem has been patched in XWiki 14.6RC1, 13.10.8 and 14.4.3. The patch (commit `2fc20891`) for the document `Menu.MenuMacro` can be manually applied or a XAR archive of a patched version can be imported. The menu macro was basically unchanged since XWiki 11.6 so on XWiki 11.6 or later the patch for version of 13.10.8 (commit `59ccca24a`) can most likely be applied, on XWiki version 14.0 and later the versions in XWiki 14.6 and 14.4.3 should be appropriate.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41931	xwiki-platform-icon-ui is vulnerable to Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection'). Any user with view rights on commonly accessible documents including the icon picker macro can execute arbitrary Groovy, Python or Velocity code in XWiki due to improper neutralization of the macro parameters of the icon picker macro. The problem has been patched in XWiki 13.10.7, 14.5 and 14.4.2. Workarounds: The [patch](https://github.com/xwiki/xwiki-platform/commit/47eb8a5fba550f477944eb6da8ca91b87eaf1d01) can be manually applied by editing `IconThemesCode.IconPickerMacro` in the object editor. The whole document can also be replaced by the current version by importing the document from the XAR archive of a fixed version as the only changes to the document have been security fixes and small formatting changes.	9.9	More Details
CVE-2022-41928	XWiki Platform vulnerable to Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') in AttachmentSelector.xml. The issue can also be reproduced by inserting the dangerous payload in the `height` or `alt` macro properties. This has been patched in versions 13.10.7, 14.4.2, and 14.5. The issue can be fixed on a running wiki by updating `XWiki.AttachmentSelector` with the versions below: - 14.5-rc-1+: https://github.com/xwiki/xwiki-platform/commit/eb15147adf94bddb92626f862c1710d45bcd64a7#diff-e1513599ab698991f6cbba55d38f3f464432ced8d137a668b1f7618c7e747e23 - 14.4.2+: https://github.com/xwiki/xwiki-platform/commit/c02f8eb1f3c953d124f2c097021536f8bc00fa8d#diff-e1513599ab698991f6cbba55d38f3f464432ced8d137a668b1f7618c7e747e23 - 13.10.7+: https://github.com/xwiki/xwiki-platform/commit/efd0df0468d46149ba68b66660b93f31b6318515#diff-e1513599ab698991f6cbba55d38f3f464432ced8d137a668b1f7618c7e747e23	9.9	More Details
CVE-2022-45908	In PaddlePaddle before 2.4, paddle.audio.functional.get_window is vulnerable to code injection because it calls eval on a user-supplied winstr. This may lead to arbitrary code execution.	9.8	More Details
CVE-2022-45206	Jeecg-boot v3.4.3 was discovered to contain a SQL injection vulnerability via the component /sys/duplicate/check.	9.8	More Details
CVE-2022-45207	Jeecg-boot v3.4.3 was discovered to contain a SQL injection vulnerability via the component updateNullByEmptyString.	9.8	More Details
CVE-2022-41705	Badaso version 2.6.3 allows an unauthenticated remote attacker to execute arbitrary code remotely on the server. This is possible because the application does not properly validate the data uploaded by users.	9.8	More Details
CVE-2022-45476	Tiny File Manager version 2.4.8 executes the code of files uploaded by users of the application, instead of just returning them for download. This is possible because the application is vulnerable to insecure file upload.	9.8	More Details
CVE-2022-44843	TOTOlink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability via the port parameter in the setting/setOpenVpnClientCfg function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44844	TOTOlink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability via the pass parameter in the setting/setOpenVpnCfg function.	9.8	More Details
CVE-2022-45907	In PyTorch before trunk/89695, torch.jit.annotations.parse_type_line can cause arbitrary code execution because eval is used unsafely.	9.8	More Details
CVE-2020-23583	OPTILINK OP-XT71000N V2.2 is vulnerable to Remote Code Execution. The issue occurs when the attacker sends an arbitrary code on "/diag_ping_admin.asp" to "PingTest" interface that leads to COMMAND EXECUTION. An attacker can successfully trigger the COMMAND and can compromise full system.	9.8	More Details
CVE-2022-2650	Improper Restriction of Excessive Authentication Attempts in GitHub repository wger-project/wger prior to 2.2.	9.8	More Details
CVE-2022-45933	KubeView through 0.1.31 allows attackers to obtain control of a Kubernetes cluster because api/scrape/kube-system does not require authentication, and retrieves certificate files that can be used for authentication as kube-admin. NOTE: the vendor's position is that KubeView was a "fun side project and a learning exercise," and not "very secure."	9.8	More Details
CVE-2022-36193	SQL injection in School Management System 1.0 allows remote attackers to modify or delete data, causing persistent changes to the application's content or behavior by using malicious SQL queries.	9.8	More Details
CVE-2022-3603	The Export customers list csv for WooCommerce, WordPress users csv, export Guest customer list WordPress plugin before 2.0.69 does not validate data when outputting it back in a CSV file, which could lead to CSV injection.	9.8	More Details
CVE-2022-44283	AVS Audio Converter 10.3 is vulnerable to Buffer Overflow.	9.8	More Details
CVE-2022-44400	Purchase Order Management System v1.0 contains a file upload vulnerability via /purchase_order/admin/?page=system_info.	9.8	More Details
CVE-2022-44401	Online Tours & Travels Management System v1.0 contains an arbitrary file upload vulnerability via /tour/admin/file.php.	9.8	More Details
CVE-2022-44399	Poultry Farm Management System v1.0 contains a SQL injection vulnerability via the del parameter at /Redcock-Farm/farm/category.php.	9.8	More Details
CVE-2022-42109	Online-shopping-system-advanced 1.0 was discovered to contain a SQL injection vulnerability via the p parameter at /shopping/product.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44038	Russound XSourcePlayer 777D v06.08.03 was discovered to contain a remote code execution vulnerability via the scriptRunner.cgi component.	9.8	More Details
CVE-2022-44354	SolarView Compact 4.0 and 5.0 is vulnerable to Unrestricted File Upload via a crafted php file.	9.8	More Details
CVE-2020-23584	Unauthenticated remote code execution in OPTILINK OP-XT71000N, Hardware Version: V2.2 occurs when the attacker passes arbitrary commands with IP-ADDRESS using "	" to execute commands on " /diag_tracert_admin.asp " in the "PingTest" parameter that leads to command execution.	9.8	More Details
CVE-2022-3751	SQL Injection in GitHub repository owncast/owncast prior to 0.0.13.	9.8	More Details
CVE-2022-44139	Apartment Visitor Management System v1.0 is vulnerable to SQL Injection via /avms/index.php.	9.8	More Details
CVE-2022-44117	Boa 0.94.14rc21 is vulnerable to SQL Injection via username. NOTE: the is disputed by multiple third parties because Boa does not ship with any support for SQL.	9.8	More Details
CVE-2022-44255	TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a pre-authentication buffer overflow in the main function via long post data.	9.8	More Details
CVE-2022-44251	TOTOLINK NR1800X V9.1.0u.6279_B20210910 contains a command injection via the ussd parameter in the setUssd function.	9.8	More Details
CVE-2021-35284	SQL Injection vulnerability in function get_user in login_manager.php in rizalafani cms-php v1.	9.8	More Details
CVE-2022-4136	Dangerous method exposed which can lead to RCE in qmpass/leadshop v1.4.15 allows an attacker to control the target host by calling any function in leadshop.php via the GET method.	9.8	More Details
CVE-2022-44250	TOTOLINK NR1800X V9.1.0u.6279_B20210910 contains a command injection via the hostName parameter in the setOpModeCfg function.	9.8	More Details
CVE-2022-44249	TOTOLINK NR1800X V9.1.0u.6279_B20210910 contains a command injection via the FileName parameter in the UploadFirmwareFile function.	9.8	More Details
CVE-2022-44252	TOTOLINK NR1800X V9.1.0u.6279_B20210910 contains a command injection via the FileName parameter in the setUploadSetting function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44118	dedecmdv6 v6.1.9 is vulnerable to Remote Code Execution (RCE) via file_manage_control.php.	9.8	More Details
CVE-2022-44120	dedecmdv6 6.1.9 is vulnerable to SQL Injection. via sys_sql_query.php.	9.8	More Details
CVE-2022-45276	An issue in the /index/user/user_edit.html component of YJCMS v1.0.9 allows unauthenticated attackers to obtain the Administrator account password.	9.8	More Details
CVE-2022-45872	iTerm2 before 3.4.18 mishandles a DECRQSS response.	9.8	More Details
CVE-2022-45462	Alarm instance management has command injection when there is a specific command configured. It is only for logged-in users. We recommend you upgrade to version 2.0.6 or higher	9.8	More Details
CVE-2022-43213	Billing System Project v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at editorder.php.	9.8	More Details
CVE-2020-23591	A vulnerability in OPTILINK OP-XT71000N Hardware Version: V2.2 , Firmware Version: OP_V3.3.1-191028 allows an attacker to upload arbitrary files through " /mgm_dev_upgrade.asp " which can "delete every file for Denial of Service (using 'rm -rf *.*' in the code), reverse connection (using '.asp' webshell), backdoor.	9.8	More Details
CVE-2022-41924	A vulnerability identified in the Tailscale Windows client allows a malicious website to reconfigure the Tailscale daemon `tailscaled`, which can then be used to remotely execute code. In the Tailscale Windows client, the local API was bound to a local TCP socket, and communicated with the Windows client GUI in cleartext with no Host header verification. This allowed an attacker-controlled website visited by the node to rebind DNS to an attacker-controlled DNS server, and then make local API requests in the client, including changing the coordination server to an attacker-controlled coordination server. An attacker-controlled coordination server can send malicious URL responses to the client, including pushing executables or installing an SMB share. These allow the attacker to remotely execute code on the node. All Windows clients prior to version v.1.32.3 are affected. If you are running Tailscale on Windows, upgrade to v1.32.3 or later to remediate the issue.	9.6	More Details
CVE-2022-4135	Heap buffer overflow in GPU in Google Chrome prior to 107.0.5304.121 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2022-41912	The crewjam/saml go library prior to version 0.4.9 is vulnerable to an authentication bypass when processing SAML responses containing multiple Assertion elements. This issue has been corrected in version 0.4.9. There are no workarounds other than upgrading to a fixed version.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29830	Use of Hard-coded Cryptographic Key vulnerability in Mitsubishi Electric GX Works3 versions from 1.000A to 1.095Z and Motion Control Setting(GX Works3 related software) versions from 1.000A and later allows a remote unauthenticated attacker to disclose or tamper with sensitive information. As a result, unauthenticated attackers may obtain information about project files illegally.	9.1	More Details
CVE-2022-43705	In Botan before 2.19.3, it is possible to forge OCSP responses due to a certificate verification error. This issue was introduced in Botan 1.11.34 (November 2016).	9.1	More Details
CVE-2022-41923	Grails Spring Security Core plugin is vulnerable to privilege escalation. The vulnerability allows an attacker access to one endpoint (i.e. the targeted endpoint) using the authorization requirements of a different endpoint (i.e. the donor endpoint). In some Grails framework applications, access to the targeted endpoint will be granted based on meeting the authorization requirements of the donor endpoint, which can result in a privilege escalation attack. This vulnerability has been patched in grails-spring-security-core versions 3.3.2, 4.0.5 and 5.1.1. Impacted Applications: Grails Spring Security Core plugin versions: 1.x 2.x >=3.0.0 <3.3.2 >=4.0.0 <4.0.5 >=5.0.0 <5.1.1 We strongly suggest that all Grails framework applications using the Grails Spring Security Core plugin be updated to a patched release of the plugin. Workarounds: Users should create a subclass extending one of the following classes from the `grails.plugin.springsecurity.web.access.intercept` package, depending on their security configuration: * `AnnotationFilterInvocationDefinition` * `InterceptUrlMapFilterInvocationDefinition` * `RequestmapFilterInvocationDefinition` In each case, the subclass should override the `calculateUri` method like so: ``` @Override protected String calculateUri(HttpServletRequest request) { UrlPathHelper.defaultInstance.getRequestUri(request) } ``` This should be considered a temporary measure, as the patched versions of grails-spring-security-core deprecates the `calculateUri` method. Once upgraded to a patched version of the plugin, this workaround is no longer needed. The workaround is especially important for version 2.x, as no patch is available version 2.x of the GSSC plugin.	9.1	More Details
CVE-2022-43196	dedecmdv6 v6.1.9 is vulnerable to Arbitrary file deletion via file_manage_control.php.	9.1	More Details
CVE-2022-45152	A blind Server-Side Request Forgery (SSRF) vulnerability was found in Moodle. This flaw exists due to insufficient validation of user-supplied input in LTI provider library. The library does not utilise Moodle's inbuilt cURL helper, which resulted in a blind SSRF risk. An attacker can send a specially crafted HTTP request and trick the application to initiate requests to arbitrary systems. This vulnerability allows a remote attacker to perform SSRF attacks.	9.1	More Details
CVE-2022-36133	The WebConfig functionality of Epson TM-C3500 and TM-C7500 devices with firmware version WAM31500 allows authentication bypass.	9.1	More Details
CVE-2022-45909	drachtio-server before 0.8.19 has a heap-based buffer over-read via a long Request-URI in an INVITE request.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37721	PyroCMS 3.9 is vulnerable to a stored Cross Site Scripting (XSS_ when a low privileged user such as an author, injects a crafted html and javascript payload in a blog post, leading to full admin account takeover or privilege escalation.	9.0	More Details
CVE-2022-37720	Orchardproject Orchard CMS 1.10.3 is vulnerable to Cross Site Scripting (XSS). When a low privileged user such as an author or publisher, injects a crafted html and javascript payload in a blog post, leading to full admin account takeover or privilege escalation when the malicious blog post is loaded in the victim's browser.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-3768	The WPSmartContracts WordPress plugin before 1.3.12 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as author	8.8	More Details
CVE-2021-43258	CartView.php in ChurchInfo 1.3.0 allows attackers to achieve remote code execution through insecure uploads. This requires authenticated access tot he ChurchInfo application. Once authenticated, a user can add names to their cart, and compose an email. Uploading an attachment for the email stores the attachment on the site in the /tmp_attach/ folder where it can be accessed with a GET request. There are no limitations on files that can be attached, allowing for malicious PHP code to be uploaded and interpreted by the server.	8.8	More Details
CVE-2022-44260	TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a post-authentication buffer overflow via parameter sPort/ePort in the setIpPortFilterRules function.	8.8	More Details
CVE-2022-31877	An issue in the component MSI.TerminalServer.exe of MSI Center v1.0.41.0 allows attackers to escalate privileges via a crafted TCP packet.	8.8	More Details
CVE-2022-3865	The WP User Merger WordPress plugin before 1.5.3 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as admin	8.8	More Details
CVE-2022-3849	The WP User Merger WordPress plugin before 1.5.3 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as admin	8.8	More Details
CVE-2022-3848	The WP User Merger WordPress plugin before 1.5.3 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as admin	8.8	More Details
CVE-2022-3769	The OWM Weather WordPress plugin before 5.6.9 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as contributor	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40282	The web server of Hirschmann BAT-C2 before 09.13.01.00R04 allows authenticated command injection. This allows an authenticated attacker to pass commands to the shell of the system because the dir parameter of the FsCreateDir Ajax function is not sufficiently sanitized. The vendor's ID is BSECV-2022-21.	8.8	More Details
CVE-2022-45278	Jizhicms v2.3.3 was discovered to contain a SQL injection vulnerability via the /index.php/admins/Fields/get_fields.html component.	8.8	More Details
CVE-2022-23044	Tiny File Manager version 2.4.8 allows an unauthenticated remote attacker to persuade users to perform unintended actions within the application. This is possible because the application is vulnerable to CSRF.	8.8	More Details
CVE-2022-44253	TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a post-authentication buffer overflow via parameter ip in the setDiagnosisCfg function.	8.8	More Details
CVE-2022-44254	TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a post-authentication buffer overflow via parameter text in the setSmsCfg function.	8.8	More Details
CVE-2022-44256	TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a post-authentication buffer overflow via parameter lang in the setLanguageCfg function.	8.8	More Details
CVE-2022-44257	TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a post-authentication buffer overflow via parameter pppoeUser in the setOpModeCfg function.	8.8	More Details
CVE-2022-44258	TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a post-authentication buffer overflow via parameter command in the setTracerouteCfg function.	8.8	More Details
CVE-2022-45442	Sinatra is a domain-specific language for creating web applications in Ruby. An issue was discovered in Sinatra 2.0 before 2.2.3 and 3.0 before 3.0.4. An application is vulnerable to a reflected file download (RFD) attack that sets the Content-Disposition header of a response when the filename is derived from user-supplied input. Version 2.2.3 and 3.0.4 contain patches for this issue.	8.8	More Details
CVE-2022-44259	TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a post-authentication buffer overflow via parameter week, sTime, and eTime in the setParentalRules function.	8.8	More Details
CVE-2022-36964	SolarWinds Platform was susceptible to the Deserialization of Untrusted Data. This vulnerability allows a remote adversary with valid access to SolarWinds Web Console to execute arbitrary commands.	8.8	More Details
CVE-2020-23585	A remote attacker can conduct a cross-site request forgery (CSRF) attack on OPTILINK OP-XT71000N Hardware Version: V2.2 , Firmware Version: OP_V3.3.1-191028. The vulnerability is due to insufficient CSRF protections for the "mgm_config_file.asp" because of which attacker can create a crafted "csrf form" which sends " malicious xml data" to "/boaform/admin/formMgmConfigUpload". the exploit allows attacker to "gain full privileges" and to "fully compromise of router & network".	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44037	An access control issue in APsystems ENERGY COMMUNICATION UNIT (ECU-C) Power Control Software V4.1NA, V3.11.4, W2.1NA, V4.1SAA, C1.2.2 allows attackers to access sensitive data and execute specific commands and functions with full admin rights without authenticating allows him to perform multiple attacks, such as attacking wireless network in the product's range.	8.8	More Details
CVE-2022-23740	CRITICAL: An improper neutralization of argument delimiters in a command vulnerability was identified in GitHub Enterprise Server that enabled remote code execution. To exploit this vulnerability, an attacker would need permission to create and build GitHub Pages using GitHub Actions. This vulnerability affected only version 3.7.0 of GitHub Enterprise Server and was fixed in version 3.7.1. This vulnerability was reported via the GitHub Bug Bounty program.	8.8	More Details
CVE-2022-40799	Data Integrity Failure in 'Backup Config' in D-Link DNR-322L <= 2.60B15 allows an authenticated attacker to execute OS level commands on the device.	8.8	More Details
CVE-2020-23592	A vulnerability in OPTILINK OP-XT71000N Hardware Version: V2.2 , Firmware Version: OP_V3.3.1-191028 allows an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack to Reset ONU to Factory Default through ' /mgm_dev_reset.asp.' Resetting to default leads to Escalation of Privileges by logging-in with default credentials.	8.8	More Details
CVE-2022-44635	Apache Fineract allowed an authenticated user to perform remote code execution due to a path traversal vulnerability in a file upload component of Apache Fineract, allowing an attacker to run remote code. This issue affects Apache Fineract version 1.8.0 and prior versions. We recommend users to upgrade to 1.8.1.	8.8	More Details
CVE-2022-44789	A logical issue in O_getOwnPropertyDescriptor() in Artifex MuJS 1.0.0 through 1.3.x before 1.3.2 allows an attacker to achieve Remote Code Execution through memory corruption, via the loading of a crafted JavaScript file.	8.8	More Details
CVE-2022-41925	A vulnerability identified in the Tailscale client allows a malicious website to access the peer API, which can then be used to access Tailscale environment variables. In the Tailscale client, the peer API was vulnerable to DNS rebinding. This allowed an attacker-controlled website visited by the node to rebind DNS for the peer API to an attacker-controlled DNS server, and then making peer API requests in the client, including accessing the node’s Tailscale environment variables. An attacker with access to the peer API on a node could use that access to read the node’s environment variables, including any credentials or secrets stored in environment variables. This may include Tailscale authentication keys, which could then be used to add new nodes to the user’s tailnet. The peer API access could also be used to learn of other nodes in the tailnet or send files via Taildrop. All Tailscale clients prior to version v1.32.3 are affected. Upgrade to v1.32.3 or later to remediate the issue.	8.8	More Details
CVE-2022-36960	SolarWinds Platform was susceptible to Improper Input Validation. This vulnerability allows a remote adversary with valid access to SolarWinds Web Console to escalate user privileges.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3898	The WP Affiliate Platform plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 6.3.9. This is due to missing or incorrect nonce validation on various functions including the affiliates_menu method. This makes it possible for unauthenticated attackers to delete affiliate records, via forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2022-3747	The Becustom plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.0.5.2. This is due to missing nonce validation when saving the plugin's settings. This makes it possible for unauthenticated attackers to update the plugin's settings like betheme_url_slug, replaced_theme_author, and betheme_label to name a few, via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2021-29334	An issue was discovered in JIZHI CMS 1.9.4. There is a CSRF vulnerability that can add an admin account via index, /admin.php/Admin/adminadd.html	8.8	More Details
CVE-2022-44140	Jizhicms v2.3.3 was discovered to contain a SQL injection vulnerability via the /Member/memberedit.html component.	8.8	More Details
CVE-2021-45036	Velneo vClient on its 28.1.3 version, could allow an attacker with knowledge of the victims's username and hashed password to spoof the victim's id against the server.	8.7	More Details
CVE-2022-25164	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric GX Works3 versions from 1.000A to 1.095Z and Mitsubishi Electric MX OPC UA Module Configurator-R versions 1.08J and prior allows a remote unauthenticated attacker to disclose sensitive information. As a result, unauthenticated attackers can gain unauthorized access to the MELSEC CPU module and the MELSEC OPC UA server module.	8.6	More Details
CVE-2022-45868	The web-based admin console in H2 Database Engine before 2.2.220 can be started via the CLI with the argument -webAdminPassword, which allows the user to specify the password in cleartext for the web admin console. Consequently, a local user (or an attacker that has obtained local access through some means) would be able to discover the password by listing processes and their arguments. NOTE: the vendor states "This is not a vulnerability of H2 Console ... Passwords should never be passed on the command line and every qualified DBA or system administrator is expected to know that." Nonetheless, the issue was fixed in 2.2.220.	8.4	More Details
CVE-2022-46147	Drag and Drop XBlock v2 implements a drag-and-drop style problem, where a learner has to drag items to zones on a target image. Versions prior to 3.0.0 are vulnerable to cross-site scripting in multiple XBlock Fields. Any platform that has deployed the XBlock may be impacted. Version 3.0.0 contains a patch for this issue. There are no known workarounds.	8.4	More Details
CVE-2022-41706	Browsershot version 3.57.2 allows an external attacker to remotely obtain arbitrary local files. This is possible because the application does not validate the URL protocol passed to the Browsershot::url method.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43984	Browsershot version 3.57.3 allows an external attacker to remotely obtain arbitrary local files. This is possible because the application does not validate that the JS content imported from an external source passed to the Browsershot::html method does not contain URLs that use the file:// protocol.	8.2	More Details
CVE-2022-43983	Browsershot version 3.57.2 allows an external attacker to remotely obtain arbitrary local files. This is possible because the application does not validate that the HTML content passed to the Browsershot::html method does not contain URL's that use the file:// protocol.	8.2	More Details
CVE-2022-46152	OP-TEE Trusted OS is the secure side implementation of OP-TEE project, a Trusted Execution Environment. Versions prior to 3.19.0, contain an Improper Validation of Array Index vulnerability. The function `cleanup_shm_refs()` is called by both `entry_invoke_command()` and `entry_open_session()`. The commands `OPTEE_MSG_CMD_OPEN_SESSION` and `OPTEE_MSG_CMD_INVOKE_COMMAND` can be executed from the normal world via an OP-TEE SMC. This function is not validating the `num_params` argument, which is only limited to `OPTEE_MSG_MAX_NUM_PARAMS` (127) in the function `get_cmd_buffer()`. Therefore, an attacker in the normal world can craft an SMC call that will cause out-of-bounds reading in `cleanup_shm_refs` and potentially freeing of fake-objects in the function `mobj_put()`. A normal-world attacker with permission to execute SMC instructions may exploit this flaw. Maintainers believe this problem permits local privilege escalation from the normal world to the secure world. Version 3.19.0 contains a fix for this issue. There are no known workarounds.	8.2	More Details
CVE-2022-36337	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. A stack buffer overflow vulnerability in the MebxConfiguration driver leads to arbitrary code execution. Control of a UEFI variable under the OS can cause this overflow when read by BIOS code.	8.2	More Details
CVE-2022-38813	PHPGurukul Blood Donor Management System 1.0 does not properly restrict access to admin/dashboard.php, which allows attackers to access all data of users, delete the users, add and manage Blood Group, and Submit Report.	8.1	More Details
CVE-2022-41922	`yiisoft/yii` before version 1.1.27 are vulnerable to Remote Code Execution (RCE) if the application calls `unserialize()` on arbitrary user input. This has been patched in 1.1.27.	8.1	More Details
CVE-2022-41157	A specific file on the sERP server if Kyungrinara(ERP solution) has a fixed password with the SYSTEM authority. This vulnerability could allow attackers to leak or steal sensitive information or execute malicious commands.	8.1	More Details
CVE-2022-4020	Vulnerability in the HQSwSmiDxe DXE driver on some consumer Acer Notebook devices may allow an attacker with elevated privileges to modify UEFI Secure Boot settings by modifying an NVRAM variable.	8.1	More Details
CVE-2022-40870	The Web Client of Parallels Remote Application Server v18.0 is vulnerable to Host Header Injection attacks. This vulnerability allows attackers to execute arbitrary commands via a crafted payload injected into the Host header.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4030	The Simple:Press plugin for WordPress is vulnerable to Path Traversal in versions up to, and including, 6.8 via the 'file' parameter which can be manipulated during user avatar deletion. This makes it possible with attackers, with minimal permissions such as a subscriber, to supply paths to arbitrary files on the server that will subsequently be deleted. This can be used to delete the wp-config.php file that can allow an attacker to configure the site and achieve remote code execution.	8.1	More Details
CVE-2022-42896	There are use-after-free vulnerabilities in the Linux kernel's net/bluetooth/l2cap_core.c's l2cap_connect and l2cap_le_connect_req functions which may allow code execution and leaking kernel memory (respectively) remotely via Bluetooth. A remote attacker could execute code leaking kernel memory via Bluetooth if within proximity of the victim. We recommend upgrading past commit https://www.google.com/url https://github.com/torvalds/linux/commit/711f8c3fb3db61897080468586b970c87c61d9e4 https://www.google.com/url	8.0	More Details
CVE-2022-41675	A remote attacker with general user privilege can inject malicious code in the form content of Raiden MAILD Mail Server website. Other users export form content as CSV file can trigger arbitrary code execution and allow the attacker to perform arbitrary system operation or disrupt service on the user side.	8.0	More Details
CVE-2022-45934	An issue was discovered in the Linux kernel through 6.0.10. l2cap_config_req in net/bluetooth/l2cap_core.c has an integer wraparound via L2CAP_CONF_REQ packets.	7.8	More Details
CVE-2022-45939	GNU Emacs through 28.2 allows attackers to execute commands via shell metacharacters in the name of a source-code file, because lib-src/etags.c uses the system C library function in its implementation of the ctags program. For example, a victim may use the "ctags *" command (suggested in the ctags documentation) in a situation where the current working directory has contents that depend on untrusted input.	7.8	More Details
CVE-2022-4141	Heap based buffer overflow in vim/vim 9.0.0946 and below by allowing an attacker to CTRL-W gf in the expression used in the RHS of the substitute command.	7.8	More Details
CVE-2022-3088	UC-8100A-ME-T System Image: Versions v1.0 to v1.6, UC-2100 System Image: Versions v1.0 to v1.12, UC-2100-W System Image: Versions v1.0 to v 1.12, UC-3100 System Image: Versions v1.0 to v1.6, UC-5100 System Image: Versions v1.0 to v1.4, UC-8100 System Image: Versions v3.0 to v3.5, UC-8100-ME-T System Image: Versions v3.0 and v3.1, UC-8200 System Image: v1.0 to v1.5, AIG-300 System Image: v1.0 to v1.4, UC-8410A with Debian 9 System Image: Versions v4.0.2 and v4.1.2, UC-8580 with Debian 9 System Image: Versions v2.0 and v2.1, UC-8540 with Debian 9 System Image: Versions v2.0 and v2.1, and DA-662C-16-LX (GLB) System Image: Versions v1.0.2 to v1.1.2 of Moxa's ARM-based computers have an execution with unnecessary privileges vulnerability, which could allow an attacker with user-level privileges to gain root privileges.	7.8	More Details
CVE-2022-45202	GPAC v2.1-DEV-rev428-gcb8ae46c8-master was discovered to contain a stack overflow via the function dimC_box_read at isomedia/box_code_3gpp.c.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45343	GPAC v2.1-DEV-rev478-g696e6f868-master was discovered to contain a heap use-after-free via the Q_IsTypeOn function at /gpac/src/bifs/unquantize.c.	7.8	More Details
CVE-2022-43751	McAfee Total Protection prior to version 16.0.49 contains an uncontrolled search path element vulnerability due to the use of a variable pointing to a subdirectory that may be controllable by an unprivileged user. This may have allowed the unprivileged user to execute arbitrary code with system privileges.	7.8	More Details
CVE-2022-40304	An issue was discovered in libxml2 before 2.10.3. Certain invalid XML entity definitions can corrupt a hash table key, potentially leading to subsequent logic errors. In one case, a double-free can be provoked.	7.8	More Details
CVE-2022-41156	Remote code execution vulnerability due to insufficient verification of URLs, etc. in OndiskPlayerAgent. A remote attacker could exploit the vulnerability to cause remote code execution by causing an arbitrary user to download and execute malicious code.	7.8	More Details
CVE-2022-38140	Auth. (contributor+) Arbitrary File Upload in SEO Plugin by Squirrly SEO plugin <= 12.1.10 on WordPress.	7.6	More Details
CVE-2022-46155	Airtable.js is the JavaScript client for Airtable. Prior to version 0.11.6, Airtable.js had a misconfigured build script in its source package. When the build script is run, it would bundle environment variables into the build target of a transpiled bundle. Specifically, the AIRTABLE_API_KEY and AIRTABLE_ENDPOINT_URL environment variables are inserted during Browserify builds due to being referenced in Airtable.js code. This only affects copies of Airtable.js built from its source, not those installed via npm or yarn. Airtable API keys set in users' environments via the AIRTABLE_API_KEY environment variable may be bundled into local copies of Airtable.js source code if all of the following conditions are met: 1) the user has cloned the Airtable.js source onto their machine, 2) the user runs the `npm prepare` script, and 3) the user' has the AIRTABLE_API_KEY environment variable set. If these conditions are met, a user's local build of Airtable.js would be modified to include the value of the AIRTABLE_API_KEY environment variable, which could then be accidentally shipped in the bundled code. Users who do not meet all three of these conditions are not impacted by this issue. Users should upgrade to Airtable.js version 0.11.6 or higher; or, as a workaround unset the AIRTABLE_API_KEY environment variable in their shell and/or remove it from your .bashrc, .zshrc, or other shell configuration files. Users should also regenerate any Airtable API keys they use, as the keysy may be present in bundled code.	7.6	More Details
CVE-2021-46854	mod_radius in ProFTPD before 1.3.7c allows memory disclosure to RADIUS servers because it copies blocks of 16 characters.	7.5	More Details
CVE-2022-25848	This affects all versions of package static-dev-server. This is because when paths from users to the root directory are joined, the assets for the path accessed are relative to that of the root directory.	7.5	More Details
CVE-2022-29831	Use of Hard-coded Password vulnerability in Mitsubishi Electric Corporation GX Works3 versions from 1.015R to 1.095Z allows a remote unauthenticated attacker to obtain information about the project file for MELSEC safety CPU modules.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45329	AeroCMS v0.0.1 was discovered to contain a SQL Injection vulnerability via the Search parameter. This vulnerability allows attackers to access database information.	7.5	More Details
CVE-2022-43326	An Insecure Direct Object Reference (IDOR) vulnerability in the password reset function of Telos Alliance Omnia MPX Node 1.0.0-1.4.[*] allows attackers to arbitrarily change user and Administrator account passwords.	7.5	More Details
CVE-2022-2721	In affected versions of Octopus Server it is possible for target discovery to print certain values marked as sensitive to log files in plaint-text in when verbose logging is enabled.	7.5	More Details
CVE-2022-41568	LINE client for iOS before 12.17.0 might be crashed by sharing an invalid shared key of e2ee in group chat.	7.5	More Details
CVE-2022-37772	Maarch RM 2.8.3 solution contains an improper restriction of excessive authentication attempts due to excessive verbose responses from the application. An unauthenticated remote attacker could potentially exploit this vulnerability, leading to compromised accounts.	7.5	More Details
CVE-2022-38166	In F-Secure Endpoint Protection for Windows and macOS before channel with Capricorn database 2022-11-22_07, the aerdl.dll unpacker handler crashes. This can lead to a scanning engine crash, triggerable remotely by an attacker for denial of service.	7.5	More Details
CVE-2022-38767	An issue was discovered in Wind River VxWorks 6.9 and 7, that allows a specifically crafted packet sent by a Radius server, may cause Denial of Service during the IP Radius access procedure.	7.5	More Details
CVE-2022-24190	The /device/acceptBind end-point for Ourphoto App version 1.4.1 does not require authentication or authorization. The user_token header is not implemented or present on this end-point. An attacker can send a request to bind their account to any users picture frame, then send a POST request to accept their own bind request, without the end-users approval or interaction.	7.5	More Details
CVE-2022-44411	Web Based Quiz System v1.0 transmits user passwords in plaintext during the authentication process, allowing attackers to obtain users' passwords via a bruteforce attack.	7.5	More Details
CVE-2022-24188	The /device/signin end-point for the Ourphoto App version 1.4.1 discloses clear-text password information for functionality within the picture frame devices. The deviceVideoCallPassword and mqttPassword are returned in clear-text. The lack of sessions management and presence of insecure direct object references allows to return password information for other end-users devices. Many of the picture frame devices offer video calling, and it is likely this information can be used to abuse that functionality.	7.5	More Details
CVE-2022-24187	The user_id and device_id on the Ourphoto App version 1.4.1 /device/* end-points both suffer from insecure direct object reference vulnerabilities. Other end-users user_id and device_id values can be enumerated by incrementing or decrementing id numbers. The impact of this vulnerability allows an attacker to discover sensitive information such as end-user email addresses, and their unique frame_token value of all other Ourphoto App end-users.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45921	FusionAuth before 1.41.3 allows a file outside of the application root to be viewed or retrieved using an HTTP request. To be specific, an attacker may be able to view or retrieve any file readable by the user running the FusionAuth process.	7.5	More Details
CVE-2022-34830	An Arm product family through 2022-06-29 has a TOCTOU Race Condition that allows non-privileged user to make improper GPU processing operations to gain access to already freed memory.	7.5	More Details
CVE-2022-41957	Muhammara is a node module with c/cpp bindings to modify PDF with JavaScript for node or electron. The package muhammara before 2.6.2 and from 3.0.0 and before 3.3.0, as well as all versions of muhammara's predecessor package hummus, are vulnerable to Denial of Service (DoS) when supplied with a maliciously crafted PDF file to be parsed. The issue has been patched in muhammara version 3.4.0 and the fix has been backported to version 2.6.2. As a workaround, do not process files from untrusted sources. If using hummus, replace the package with muhammara.	7.5	More Details
CVE-2022-38900	decode-uri-component 0.2.0 is vulnerable to Improper Input Validation resulting in DoS.	7.5	More Details
CVE-2022-45932	A SQL injection issue was discovered in AAA in OpenDaylight (ODL) before 0.16.5. The aaa-idm-store-h2/src/main/java/org/opendaylight/aaa/datastore/h2/RoleStore.java deleteRole function is affected when the API interface /auth/v1/roles/ is used.	7.5	More Details
CVE-2022-45931	A SQL injection issue was discovered in AAA in OpenDaylight (ODL) before 0.16.5. The aaa-idm-store-h2/src/main/java/org/opendaylight/aaa/datastore/h2/UserStore.java deleteUser function is affected when the API interface /auth/v1/users/ is used.	7.5	More Details
CVE-2022-45930	A SQL injection issue was discovered in AAA in OpenDaylight (ODL) before 0.16.5. The aaa-idm-store-h2/src/main/java/org/opendaylight/aaa/datastore/h2/DomainStore.java deleteDomain function is affected for the /auth/v1/domains/ API interface.	7.5	More Details
CVE-2022-26885	When using tasks to read config files, there is a risk of database password disclosure. We recommend you upgrade to version 2.0.6 or higher.	7.5	More Details
CVE-2022-24999	qs before 6.10.3, as used in Express before 4.17.3 and other products, allows attackers to cause a Node process hang for an Express application because an __ proto__ key can be used. In many typical Express use cases, an unauthenticated remote attacker can place the attack payload in the query string of the URL that is used to visit the application, such as a[__proto__]=b&a[__proto__]&a[length]=100000000. The fix was backported to qs 6.9.7, 6.8.3, 6.7.3, 6.6.1, 6.5.3, 6.4.1, 6.3.3, and 6.2.4 (and therefore Express 4.17.3, which has "deps: qs@6.9.7" in its release description, is not vulnerable).	7.5	More Details
CVE-2022-44356	WAVLINK Quantum D4G (WL-WN531G3) running firmware versions M31G3.V5030.201204 and M31G3.V5030.200325 has an access control issue which allows unauthenticated attackers to download configuration data and log files.	7.5	More Details
CVE-2022-40977	A path traversal vulnerability was discovered in Pilz PASvisu Server before 1.12.0. An unauthenticated remote attacker could use a zipped, malicious configuration file to trigger arbitrary file writes ('zip-slip'). File writes do not affect confidentiality or availability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41932	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. It's possible to make XWiki create many new schemas and fill them with tables just by using a crafted user identifier in the login form. This may lead to degraded database performance. The problem has been patched in XWiki 13.10.8, 14.6RC1 and 14.4.2. Users are advised to upgrade. There are no known workarounds for this issue.	7.5	More Details
CVE-2022-40303	An issue was discovered in libxml2 before 2.10.3. When parsing a multi-gigabyte XML document with the XML_PARSE_HUGE parser option enabled, several integer counters can overflow. This results in an attempt to access an array at a negative 2GB offset, typically leading to a segmentation fault.	7.5	More Details
CVE-2022-41930	org.xwiki.platform:xwiki-platform-user-profile-ui is missing authorization to enable or disable users. Any user (logged in or not) with access to the page XWiki.XWikiUserProfileSheet can enable or disable any user profile. This might allow to a disabled user to re-enable themselves, or to an attacker to disable any user of the wiki. The problem has been patched in XWiki 13.10.7, 14.5RC1 and 14.4.2. Workarounds: The problem can be patched immediately by editing the page `XWiki.XWikiUserProfileSheet` in the wiki and by performing the changes contained in https://github.com/xwiki/xwiki-platform/commit/5be1cc0adf917bf10899c47723fa451e950271fa.	7.5	More Details
CVE-2022-41927	XWiki Platform is vulnerable to Cross-Site Request Forgery (CSRF) that may allow attackers to delete or rename tags without needing any confirmation. The problem has been patched in XWiki 13.10.7, 14.4.1 and 14.5RC1. Workarounds: It's possible to patch existing instances directly by editing the page Main.Tags and add this kind of check, in the code for renaming and for deleting: ``` #if (!$services.csrf.isTokenValid($request.get('form_token'))) #set ($discard = $response.sendError(401, "Wrong CSRF token")) #end ```	7.4	More Details
CVE-2022-41958	super-xray is a web vulnerability scanning tool. Versions prior to 0.7 assumed trusted input for the program config which is stored in a yaml file. An attacker with local access to the file could exploit this and compromise the program. This issue has been addressed in commit `4d0d5966` and will be included in future releases. Users are advised to upgrade. There are no known workarounds for this issue.	7.3	More Details
CVE-2022-4088	A vulnerability was found in rickxy Stock Management System and classified as critical. Affected by this issue is some unknown functionality of the file /pages/processlogin.php. The manipulation of the argument user/password leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-214322 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2022-21126	The package com.github.samtools:htsjdk before 3.0.1 are vulnerable to Creation of Temporary File in Directory with Insecure Permissions due to the createTempDir() function in util/IOUtil.java not checking for the existence of the temporary directory before attempting to create it.	7.3	More Details
CVE-2022-44859	Automotive Shop Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /asms/admin/products/manage_product.php.	7.2	More Details
CVE-2022-44858	Automotive Shop Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /asms/products/view_product.php.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44860	Automotive Shop Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/transactions/update_status.php.	7.2	More Details
CVE-2022-3383	The Ultimate Member plugin for WordPress is vulnerable to Remote Code Execution in versions up to, and including, 2.5.0 via the get_option_value_from_callback function that accepts user supplied input and passes it through call_user_func(). This makes it possible for authenticated attackers, with administrative capabilities, to execute code on the server.	7.2	More Details
CVE-2022-3490	The Checkout Field Editor (Checkout Manager) for WooCommerce WordPress plugin before 1.8.0 unserializes user input provided via the settings, which could allow high privilege users such as admin to perform PHP Object Injection when a suitable gadget is present	7.2	More Details
CVE-2022-3689	The HTML Forms WordPress plugin before 1.3.25 does not properly properly escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users	7.2	More Details
CVE-2022-4032	The Quiz and Survey Master plugin for WordPress is vulnerable to iFrame Injection via the 'question[id]' parameter in versions up to, and including, 8.0.4 due to insufficient input sanitization and output escaping that allowed iframe tags to be injected. This makes it possible for unauthenticated attackers to inject iFrames in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2022-40770	Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to authenticated command injection. This can be exploited by high-privileged users.	7.2	More Details
CVE-2022-4035	The Appointment Hour Booking plugin for WordPress is vulnerable to iFrame Injection via the ‘email’ or general field parameters in versions up to, and including, 1.3.72 due to insufficient input sanitization and output escaping that makes injecting iFrame tags possible. This makes it possible for unauthenticated attackers to inject iFrames when submitting a booking that will execute whenever a user accesses the injected booking details page.	7.2	More Details
CVE-2022-44278	Sanitization Management System v1.0 is vulnerable to SQL Injection via /php-sms/admin/?page=user/manage_user&id=.	7.2	More Details
CVE-2022-39833	FileCloud Versions 20.2 and later allows remote attackers to potentially cause unauthorized remote code execution and access to reported API endpoints via a crafted HTTP request.	7.2	More Details
CVE-2022-45039	An arbitrary file upload vulnerability in the Server Settings module of WBCE CMS v1.5.4 allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4027	The Simple:Press plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'postitem' parameter manipulated during a forum response in versions up to, and including, 6.8 due to insufficient input sanitization and output escaping that makes injecting object and embed tags possible. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages when responding to forum threads that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2022-3384	The Ultimate Member plugin for WordPress is vulnerable to Remote Code Execution in versions up to, and including, 2.5.0 via the populate_dropdown_options function that accepts user supplied input and passes it through call_user_func(). This is restricted to non-parameter PHP functions like phpinfo(); since user supplied parameters are not passed through the function. This makes it possible for authenticated attackers, with administrative privileges, to execute code on the server.	7.2	More Details
CVE-2022-41158	Remote code execution vulnerability can be achieved by using cookie values as paths to a file by this builder program. A remote attacker could exploit the vulnerability to execute or inject malicious code.	7.2	More Details
CVE-2022-36962	SolarWinds Platform was susceptible to Command Injection. This vulnerability allows a remote adversary with complete control over the SolarWinds database to execute arbitrary commands.	7.2	More Details
CVE-2022-44748	A directory traversal vulnerability in the ZIP archive extraction routines of KNIME Server since 4.3.0 can result in arbitrary files being overwritten on the server's file system. This vulnerability is also known as 'Zip-Slip'. An attacker can create a KNIME workflow that, when being uploaded, can overwrite arbitrary files that the operating system user running the KNIME Server process has write access to. The user must be authenticated and have permissions to upload files to KNIME Server. This can impact data integrity (file contents are changed) or cause errors in other software (vital files being corrupted). It can even lead to remote code execution if executable files are being replaced and subsequently executed by the KNIME Server process user. In all cases the attacker has to know the location of files on the server's file system, though. Note that users that have permissions to upload workflows usually also have permissions to run them on the KNIME Server and can therefore already execute arbitrary code in the context of the KNIME Executor's operating system user. There is no workaround to prevent this vulnerability from being exploited. Updates to fixed versions 4.13.6, 4.14.3, or 4.15.3 are advised.	7.1	More Details
CVE-2022-46148	Discourse is an open-source messaging platform. In versions 2.8.10 and prior on the `stable` branch and versions 2.9.0.beta11 and prior on the `beta` and `tests-passed` branches, users composing malicious messages and navigating to drafts page could self-XSS. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse’s default Content Security Policy. This issue is patched in the latest stable, beta and tests-passed versions of Discourse.	7.1	More Details
CVE-2022-45919	An issue was discovered in the Linux kernel through 6.0.10. In drivers/media/dvb-core/dvb_ca_en50221.c, a use-after-free can occur is there is a disconnect after an open, because of the lack of a wait_event.	7.0	More Details
CVE-2022-45884	An issue was discovered in the Linux kernel through 6.0.9. drivers/media/dvb-core/dvbdev.c has a use-after-free, related to dvb_register_device dynamically allocating fops.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45885	An issue was discovered in the Linux kernel through 6.0.9. drivers/media/dvb-core/dvb_frontend.c has a race condition that can cause a use-after-free when a device is disconnected.	7.0	More Details
CVE-2009-1143	An issue was discovered in open-vm-tools 2009.03.18-154848. Local users can bypass intended access restrictions on mounting shares via a symlink attack that leverages a realpath race condition in mount.vmhgfs (aka hgfsmounter).	7.0	More Details
CVE-2022-45886	An issue was discovered in the Linux kernel through 6.0.9. drivers/media/dvb-core/dvb_net.c has a .disconnect versus dvb_device_open race condition that leads to a use-after-free.	7.0	More Details
CVE-2022-29829	Use of Hard-coded Cryptographic Key vulnerability in Mitsubishi Electric GX Works3 versions from 1.000A to 1.090U, GT Designer3 Version1 (GOT2000) versions from 1.122C to 1.290C and Motion Control Setting(GX Works3 related software) versions from 1.035M to 1.042U allows a remote unauthenticated attacker to disclose sensitive information. As a result, unauthenticated users may view programs and project files or execute programs illegally.	6.8	More Details
CVE-2022-29826	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric GX Works3 versions from 1.000A to 1.087R and Motion Control Setting(GX Works3 related software) versions from 1.000A to 1.042U allows a remote unauthenticated attacker to disclose sensitive information. As a result, unauthenticated users may view programs and project files or execute programs illegally.	6.8	More Details
CVE-2022-29827	Use of Hard-coded Cryptographic Key vulnerability in Mitsubishi Electric GX Works3 versions from 1.000A and later allows a remote unauthenticated attacker to disclose sensitive information. As a result, unauthenticated attackers may view programs and project files or execute programs illegally.	6.8	More Details
CVE-2022-29828	Use of Hard-coded Cryptographic Key vulnerability in Mitsubishi Electric GX Works3 versions from 1.000A and later allows a remote unauthenticated attacker to disclose sensitive information. As a result, unauthenticated attackers may view programs and project file or execute programs illegally.	6.8	More Details
CVE-2022-29833	Insufficiently Protected Credentials vulnerability in Mitsubishi Electric Corporation GX Works3 versions 1.015R and later allows a remote unauthenticated attacker to disclose sensitive information. As a result, unauthenticated users could access to MELSEC safety CPU modules illgally.	6.8	More Details
CVE-2009-1142	An issue was discovered in open-vm-tools 2009.03.18-154848. Local users can gain privileges via a symlink attack on /tmp files if vmware-user-suid-wrapper is setuid root and the ChmodChownDirectory function is enabled.	6.7	More Details
CVE-2022-3511	The Awesome Support WordPress plugin before 6.1.2 does not ensure that the exported tickets archive to be downloaded belongs to the user making the request, allowing a low privileged user, such as subscriber to download arbitrary exported tickets via an IDOR vector	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-23593	A vulnerability in OPTILINK OP-XT71000N Hardware Version: V2.2, Firmware Version: OP_V3.3.1-191028 allows an unauthenticated, remote attacker to conduct a cross site request forgery (CSRF) attack to enable syslog mode through ' /mgm_log_cfg.asp.' The system starts to log events, 'Remote' mode or 'Both' mode on "Syslog -- Configuration page" logs events and sends to remote syslog server IP and Port.	6.5	More Details
CVE-2022-32966	RTL8168FP-CG Dash remote management function has missing authorization. An unauthenticated attacker within the adjacent network can connect to DASH service port to disrupt service.	6.5	More Details
CVE-2022-44937	Bosscms v2.0.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via the Add function under the Administrator List module.	6.5	More Details
CVE-2020-23590	A vulnerability in Optilink OP-XT71000N Hardware version: V2.2 , Firmware Version: OP_V3.3.1-191028 allows an unauthenticated remote attacker to conduct a cross-site request forgery (CSRF) attack to change the Password for "WLAN SSID" through "wlwpa.asp".	6.5	More Details
CVE-2022-24189	The user_token authorization header on the Ourphoto App version 1.4.1 /apiv1/* end-points is not implemented properly. Removing the value causes all requests to succeed, bypassing authorization and session management. The impact of this vulnerability allows an attacker POST api calls with other users unique identifiers and enumerate information of all other end-users.	6.5	More Details
CVE-2021-31693	The 10Web Photo Gallery plugin through 1.5.68 for WordPress allows XSS via album_gallery_id_0, bwg_album_search_0, and type_0 for bwg_frontend_data. NOTE: other parameters are covered by CVE-2021-24291, CVE-2021-25041, and CVE-2021-46889. NOTE: VMware information, previously connected to this CVE ID because of a typo, is at CVE-2022-31693.	6.5	More Details
CVE-2022-4144	An out-of-bounds read flaw was found in the QXL display device emulation in QEMU. The qxl_phys2virt() function does not check the size of the structure pointed to by the guest physical address, potentially reading past the end of the bar space into adjacent pages. A malicious guest user could use this flaw to crash the QEMU process on the host causing a denial of service condition.	6.5	More Details
CVE-2022-4172	An integer overflow and buffer overflow issues were found in the ACPI Error Record Serialization Table (ERST) device of QEMU in the read_erst_record() and write_erst_record() functions. Both issues may allow the guest to overrun the host buffer allocated for the ERST memory device. A malicious guest could use these flaws to crash the QEMU process on the host.	6.5	More Details
CVE-2020-23589	A vulnerability in OPTILINK OP-XT71000N Hardware Version: V2.2 , Firmware Version: OP_V3.3.1-191028 allows an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack to cause a Denial of Service by Rebooting the router through " /mgm_dev_reboot.asp."	6.5	More Details
CVE-2022-45914	The ESL (Electronic Shelf Label) protocol, as implemented by (for example) the OV80e934802 RF transceiver on the ETAG-2130-V4.3 20190629 board, does not use authentication, which allows attackers to change label values via 433 MHz RF signals, as demonstrated by disrupting the organization of a hospital storage unit, or changing retail pricing.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4169	The Theme and plugin translation for Polylang is vulnerable to authorization bypass in versions up to, and including, 3.2.16 due to missing capability checks in the process_polylang_theme_translation_wp_loaded() function. This makes it possible for unauthenticated attackers to update plugin and theme translation settings and to import translation strings.	6.5	More Details
CVE-2022-40772	Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to a validation bypass that allows users to access sensitive data via the report module.	6.5	More Details
CVE-2022-37773	An authenticated SQL Injection vulnerability in the statistics page (/statistics/retrieve) of Maarch RM 2.8, via the filter parameter, allows the complete disclosure of all databases.	6.5	More Details
CVE-2022-41712	Frappe version 14.10.0 allows an external attacker to remotely obtain arbitrary local files. This is possible because the application does not correctly validate the information injected by the user in the import_file parameter.	6.5	More Details
CVE-2022-44280	Automotive Shop Management System v1.0 is vulnerable to Delete any file via /asms/classes/Master.php?f=delete_img.	6.5	More Details
CVE-2022-45475	Tiny File Manager version 2.4.8 allows an unauthenticated remote attacker to access the application's internal files. This is possible because the application is vulnerable to broken access control.	6.5	More Details
CVE-2022-45888	An issue was discovered in the Linux kernel through 6.0.9. drivers/char/xillybus/xillyusb.c has a race condition and use-after-free during physical removal of a USB device.	6.4	More Details
CVE-2022-4028	The Simple:Press plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'postitem' parameter manipulated during the profile-save action when modifying a profile signature in versions up to, and including, 6.8 due to insufficient input sanitization and output escaping that makes injecting object and embed tags possible. This makes it possible for authenticated attackers, with minimal permissions, such as a subscriber to inject arbitrary web scripts in pages when modifying a profile signature that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2022-3991	The Photospace Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via its settings parameters saved via the update() function in versions up to, and including, 2.3.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-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-2022-38753	This update resolves a multi-factor authentication bypass attack	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4202	A vulnerability, which was classified as problematic, was found in GPAC 2.1-DEV-rev490-g68064e101-master. Affected is the function lsr_translate_coords of the file laser/lsr_dec.c. The manipulation leads to integer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The name of the patch is b3d821c4ae9ba62b3a194d9dcb5e99f17bd56908. It is recommended to apply a patch to fix this issue. VDB-214518 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-46146	Prometheus Exporter Toolkit is a utility package to build exporters. Prior to versions 0.7.2 and 0.8.2, if someone has access to a Prometheus web.yml file and users' bcrypted passwords, they can bypass security by poisoning the built-in authentication cache. Versions 0.7.2 and 0.8.2 contain a fix for the issue. There is no workaround, but attacker must have access to the hashed password to use this functionality.	6.2	More Details
CVE-2022-41933	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. When the `reset a forgotten password` feature of XWiki was used, the password was then stored in plain text in database. This only concerns XWiki 13.1RC1 and newer versions. Note that it only concerns the reset password feature available from the "Forgot your password" link in the login view: the features allowing a user to change their password, or for an admin to change a user password are not impacted. This vulnerability is particularly dangerous in combination with other vulnerabilities allowing to perform data leak of personal data from users, such as GHSA-599v-w48h-rjrm. Note that this vulnerability only concerns the users of the main wiki: in case of farms, the users registered on subwiki are not impacted thanks to a bug we discovered when investigating this. The problem has been patched in version 14.6RC1, 14.4.3 and 13.10.8. The patch involves a migration of the impacted users as well as the history of the page, to ensure no password remains in plain text in the database. This migration also involves to inform the users about the possible disclosure of their passwords: by default, two emails are automatically sent to the impacted users. A first email to inform about the possibility that their password have been leaked, and a second email using the reset password feature to ask them to set a new password. It's also possible for administrators to set some properties for the migration: it's possible to decide if the user password should be reset (default) or if the passwords should be kept but only hashed. Note that in the first option, the users won't be able to login anymore until they set a new password if they were impacted. Note that in both options, mails will be sent to users to inform them and encourage them to change their passwords.	6.2	More Details
CVE-2022-41732	IBM Maximo Mobile 8.7 and 8.8 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 237407.	6.2	More Details
CVE-2022-36433	The blog-post creation functionality in the Amasty Blog Pro 2.10.3 plugin for Magento 2 allows injection of JavaScript code in the short_content and full_content fields, leading to XSS attacks against admin panel users via posts/preview or posts/save.	6.1	More Details
CVE-2022-2311	The Find and Replace All WordPress plugin before 1.3 does not sanitize and escape some parameters from its setting page before outputting them back to the user, leading to a Reflected Cross-Site Scripting issue.	6.1	More Details
CVE-2022-38114	This vulnerability occurs when a web server fails to correctly process the Content-Length of POST requests. This can lead to HTTP request smuggling or XSS.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44355	SolarView Compact 7.0 is vulnerable to Cross-site Scripting (XSS) via /network_test.php.	6.1	More Details
CVE-2022-44279	Garage Management System v1.0 is vulnerable to Cross Site Scripting (XSS) via /garage/php_action/createBrand.php.	6.1	More Details
CVE-2022-3847	The Showing URL in QR Code WordPress plugin through 0.0.1 does not have CSRF check when updating its settings, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin or editor add Stored XSS payloads via a CSRF attack	6.1	More Details
CVE-2022-45218	Human Resource Management System v1.0.0 was discovered to contain a cross-site scripting (XSS) vulnerability. This vulnerability is triggered via a crafted payload injected into an authentication error message.	6.1	More Details
CVE-2022-3896	The WP Affiliate Platform plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via $_SERVER["REQUEST_URI"] in versions up to, and including, 6.3.9 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. This is unlikely to work in modern browsers.	6.1	More Details
CVE-2022-0698	Microweber version 1.3.1 allows an unauthenticated user to perform an account takeover via an XSS on the 'select-file' parameter.	6.1	More Details
CVE-2022-45150	A reflected cross-site scripting vulnerability was discovered in Moodle. This flaw exists due to insufficient sanitization of user-supplied data in policy tool. An attacker can trick the victim to open a specially crafted link that executes an arbitrary HTML and script code in user's browser in context of vulnerable website. This vulnerability may allow an attacker to perform cross-site scripting (XSS) attacks to gain access potentially sensitive information and modification of web pages.	6.1	More Details
CVE-2022-45214	A cross-site scripting (XSS) vulnerability in Sanitization Management System v1.0.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the username parameter at /php-sms/classes/Login.php.	6.1	More Details
CVE-2022-45225	Book Store Management System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in /bsms_ci/index.php/book. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the book_title parameter.	6.1	More Details
CVE-2022-4034	The Appointment Hour Booking Plugin for WordPress is vulnerable to CSV Injection in versions up to, and including, 1.3.72. This makes it possible for unauthenticated attackers to embed untrusted input into content during booking creation that may be exported as a CSV file when a site's administrator exports booking details. This can result in code execution when these files are downloaded and opened on a local system with a vulnerable configuration.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41965	Opencast is a free, open-source platform to support the management of educational audio and video content. Prior to Opencast 12.5, Opencast's Paella authentication page could be used to redirect to an arbitrary URL for authenticated users. The vulnerability allows attackers to redirect users to sites outside of one's Opencast install, potentially facilitating phishing attacks or other security issues. This issue is fixed in Opencast 12.5 and newer.	5.7	More Details
CVE-2022-29825	Use of Hard-coded Password vulnerability in Mitsubishi Electric GX Works3 versions from 1.000A to 1.090U and GT Designer3 Version1 (GOT2000) versions from 1.122C to 1.290C allows an unauthenticated attacker to disclose sensitive information. As a result, unauthenticated users may view programs and project files or execute programs illegally.	5.6	More Details
CVE-2022-43589	A null pointer dereference vulnerability exists in the handle_ioctl_8314C functionality of Callback technologies CBFS Filter 20.0.8317. A specially crafted I/O request packet (IRP) can lead to denial of service. An attacker can issue an ioctl to trigger this vulnerability.	5.5	More Details
CVE-2022-44749	A directory traversal vulnerability in the ZIP archive extraction routines of KNIME Analytics Platform 3.2.0 and above can result in arbitrary files being overwritten on the user's system. This vulnerability is also known as 'Zip-Slip'. An attacker can create a KNIME workflow that, when being opened by a user, can overwrite arbitrary files that the user has write access to. It's not necessary to execute the workflow, opening the workflow is sufficient. The user will notice that something is wrong because an error is being reported but only after the files have already been written. This can impact data integrity (file contents are changed) or cause errors in other software (vital files being corrupted). It can even lead to remote code execution if executable files are being replaced and subsequently executed by the user. In all cases the attacker has to know the location of files on the user's system, though.	5.5	More Details
CVE-2022-45873	systemd 250 and 251 allows local users to achieve a systemd-coredump deadlock by triggering a crash that has a long backtrace. This occurs in parse_elf_object in shared/elf-util.c. The exploitation methodology is to crash a binary calling the same function recursively, and put it in a deeply nested directory to make its backtrace large enough to cause the deadlock. This must be done 16 times when MaxConnections=16 is set for the systemd/units/systemd-coredump.socket file.	5.5	More Details
CVE-2022-45204	GPAC v2.1-DEV-rev428-gcb8ae46c8-master was discovered to contain a memory leak via the function dimC_box_read at isomedia/box_code_3gpp.c.	5.5	More Details
CVE-2022-3897	The WP Affiliate Platform plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several parameters in versions up to, and including, 6.3.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.5	More Details
CVE-2022-4129	A flaw was found in the Linux kernel's Layer 2 Tunneling Protocol (L2TP). A missing lock when clearing sk_user_data can lead to a race condition and NULL pointer dereference. A local user could use this flaw to potentially crash the system causing a denial of service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4128	A NULL pointer dereference issue was discovered in the Linux kernel in the MPTCP protocol when traversing the subflow list at disconnect time. A local user could use this flaw to potentially crash the system causing a denial of service.	5.5	More Details
CVE-2022-4127	A NULL pointer dereference issue was discovered in the Linux kernel in io_files_update_with_index_alloc. A local user could use this flaw to potentially crash the system causing a denial of service.	5.5	More Details
CVE-2022-4104	A loop with an unreachable exit condition can be triggered by passing a crafted JPEG file to the Lepton image compression tool, resulting in a denial-of-service.	5.5	More Details
CVE-2022-43588	A null pointer dereference vulnerability exists in the handle_ioctl_83150 functionality of Callback technologies CBFS Filter 20.0.8317. A specially crafted I/O request packet (IRP) can lead to denial of service. An attacker can issue an ioctl to trigger this vulnerability.	5.5	More Details
CVE-2022-40976	A path traversal vulnerability was discovered in multiple Pilz products. An unauthenticated local attacker could use a zipped, malicious configuration file to trigger arbitrary file writes ('zip-slip'). File writes do not affect confidentiality or availability.	5.5	More Details
CVE-2022-43590	A null pointer dereference vulnerability exists in the handle_ioctl_0x830a0_systembuffer functionality of Callback technologies CBFS Filter 20.0.8317. A specially crafted I/O request packet (IRP) can lead to denial of service. An attacker can issue an ioctl to trigger this vulnerability.	5.5	More Details
CVE-2022-45036	A cross-site scripting (XSS) vulnerability in the Search Settings module of WBCE CMS v1.5.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the No Results field.	5.4	More Details
CVE-2022-37421	Silverstripe silverstripe/cms through 4.11.0 allows XSS.	5.4	More Details
CVE-2022-41676	Raiden MAILD Mail Server website mail field has insufficient filtering for user input. A remote attacker with general user privilege can send email using the website with malicious JavaScript in the input field, which triggers XSS (Reflected Cross-Site Scripting) attack to the mail recipient.	5.4	More Details
CVE-2022-42099	KLiK SocialMediaWebsite Version 1.0.1 has XSS vulnerabilities that allow attackers to store XSS via location Forum Subject input.	5.4	More Details
CVE-2022-42100	KLiK SocialMediaWebsite Version 1.0.1 has XSS vulnerabilities that allow attackers to store XSS via location input reply-form.	5.4	More Details
CVE-2022-37430	Silverstripe silverstripe/framework through 4.11 allows XSS vulnerability via href attribute of a link (issue 2 of 2).	5.4	More Details
CVE-2022-37429	Silverstripe silverstripe/framework through 4.11 allows XSS (issue 1 of 2) via JavaScript payload to the href attribute of a link by splitting a javascript URL with white space characters.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38145	Silverstripe silverstripe/framework through 4.11 allows XSS (issue 1 of 3) via remote attackers adding a Javascript payload to a page's meta description and get it executed in the versioned history compare view.	5.4	More Details
CVE-2022-45149	A vulnerability was found in Moodle which exists due to insufficient validation of the HTTP request origin in course redirect URL. A user's CSRF token was unnecessarily included in the URL when being redirected to a course they have just restored. A remote attacker can trick the victim to visit a specially crafted web page and perform arbitrary actions on behalf of the victim on the vulnerable website. This flaw allows an attacker to perform cross-site request forgery attacks.	5.4	More Details
CVE-2022-35500	Amasty Blog 2.10.3 is vulnerable to Cross Site Scripting (XSS) via leave comment functionality.	5.4	More Details
CVE-2022-45280	A cross-site scripting (XSS) vulnerability in the Url parameter in /login.php of EyouCMS v1.6.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	5.4	More Details
CVE-2022-45037	A cross-site scripting (XSS) vulnerability in /admin/users/index.php of WBCE CMS v1.5.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Display Name field.	5.4	More Details
CVE-2022-45038	A cross-site scripting (XSS) vulnerability in /admin/settings/save.php of WBCE CMS v1.5.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Website Footer field.	5.4	More Details
CVE-2022-35501	Stored Cross-site Scripting (XSS) exists in the Amasty Blog Pro 2.10.3 and 2.10.4 plugin for Magento 2 because of the duplicate post function.	5.4	More Details
CVE-2022-45040	A cross-site scripting (XSS) vulnerability in /admin/pages/sections_save.php of WBCE CMS v1.5.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name Section field.	5.4	More Details
CVE-2022-36111	immudb is a database with built-in cryptographic proof and verification. In versions prior to 1.4.1, a malicious immudb server can provide a falsified proof that will be accepted by the client SDK signing a falsified transaction replacing the genuine one. This situation can not be triggered by a genuine immudb server and requires the client to perform a specific list of verified operations resulting in acceptance of an invalid state value. This vulnerability only affects immudb client SDKs, the immudb server itself is not affected by this vulnerability. This issue has been patched in version 1.4.1.	5.4	More Details
CVE-2022-45472	CAE LearningSpace Enterprise (with Intuity License) image 267r patch 639 allows DOM XSS, related to ontouchmove and onpointerup.	5.4	More Details
CVE-2022-41446	An access control issue in /Admin/dashboard.php of Record Management System using CodeIgniter v1.0 allows attackers to access and modify user data.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38724	Silverstripe silverstripe/framework through 4.11.0, silverstripe/assets through 1.11.0, and silverstripe/asset-admin through 1.11.0 allow XSS.	5.4	More Details
CVE-2022-45151	The stored-XSS vulnerability was discovered in Moodle which exists due to insufficient sanitization of user-supplied data in several "social" user profile fields. An attacker could inject and execute arbitrary HTML and script code in user's browser in context of vulnerable website.	5.4	More Details
CVE-2022-38147	Silverstripe silverstripe/framework through 4.11 allows XSS (issue 3 of 3).	5.4	More Details
CVE-2022-44284	Dinstar FXO Analog VoIP Gateway DAG2000-16O is vulnerable to Cross Site Scripting (XSS).	5.4	More Details
CVE-2022-41935	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Users without the right to view documents can deduce their existence by repeated Livetable queries. The issue has been patched in XWiki 14.6RC1, 13.10.8, and 14.4.3, the response is not properly cleaned up of obfuscated entries. As a workaround, The patch for the document `XWiki.LiveTableResultsMacros` can be manually applied or a XAR archive of a patched version can be imported, on versions 12.10.11, 13.9-rc-1, and 13.4.4. There are no known workarounds for this issue.	5.3	More Details
CVE-2022-45866	qpress before PierreLvx/qpress 20220819 and before version 11.3, as used in Percona XtraBackup and other products, allows directory traversal via ../ in a .qp file.	5.3	More Details
CVE-2022-4033	The Quiz and Survey Master plugin for WordPress is vulnerable to input validation bypass via the 'question[id]' parameter in versions up to, and including, 8.0.4 due to insufficient input validation that allows attackers to inject content other than the specified value (i.e. a number, file path, etc..). This makes it possible attackers to submit values other than the intended input type.	5.3	More Details
CVE-2022-4036	The Appointment Hour Booking plugin for WordPress is vulnerable to CAPTCHA bypass in versions up to, and including, 1.3.72. This is due to the use of insufficiently strong hashing algorithm on the CAPTCHA secret that is also displayed to the user via a cookie.	5.3	More Details
CVE-2022-45205	Jeecg-boot v3.4.3 was discovered to contain a SQL injection vulnerability via the component /sys/dict/queryTableData.	5.3	More Details
CVE-2022-40266	Improper Input Validation vulnerability in Mitsubishi Electric GOT2000 Series GT27 model FTP server versions 01.39.000 and prior, Mitsubishi Electric GOT2000 Series GT25 model FTP server versions 01.39.000 and prior and Mitsubishi Electric GOT2000 Series GT23 model FTP server versions 01.39.000 and prior allows a remote authenticated attacker to cause a Denial of Service condition by sending specially crafted command.	5.3	More Details
CVE-2022-38113	This vulnerability discloses build and services versions in the server response header.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38115	Insecure method vulnerability in which allowed HTTP methods are disclosed. E.g., OPTIONS, DELETE, TRACE, and PUT	5.3	More Details
CVE-2021-35246	The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption and use the application as a platform for attacks against its users.	5.3	More Details
CVE-2022-37774	There is a broken access control vulnerability in the Maarch RM 2.8.3 solution. When accessing some specific document (pdf, email) from an archive, a preview is proposed by the application. This preview generates a URL including an md5 hash of the file accessed. The document's URL (https://{url}/tmp/{MD5 hash of the document}) is then accessible without authentication.	5.3	More Details
CVE-2022-42895	There is an infoleak vulnerability in the Linux kernel's net/bluetooth/l2cap_core.c's l2cap_parse_conf_req function which can be used to leak kernel pointers remotely. We recommend upgrading past commit https://github.com/torvalds/linux/commit/b1a2cd50c0357f243b7435a732b4e62ba3157a2e https://www.google.com/url	5.1	More Details
CVE-2022-40771	Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to an XML External Entity attack that leads to Information Disclosure.	4.9	More Details
CVE-2022-41929	org.xwiki.platform:xwiki-platform-oldcore is missing authorization in User#setDisabledStatus, which may allow an incorrectly authorized user with only Script rights to enable or disable a user. This operation is meant to only be available for users with admin rights. This problem has been patched in XWiki 13.10.7, 14.4.2 and 14.5RC1.	4.9	More Details
CVE-2022-3601	The Image Hover Effects Css3 WordPress plugin through 4.5 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2022-3610	The Jeeng Push Notifications WordPress plugin before 2.0.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-36137	ChurchCRM Version 4.4.5 has XSS vulnerabilities that allow attackers to store XSS via location input sHeader.	4.8	More Details
CVE-2022-36136	ChurchCRM Version 4.4.5 has XSS vulnerabilities that allow attackers to store XSS via location input Deposit Comment.	4.8	More Details
CVE-2022-3839	The Analytics for WP WordPress plugin through 1.5.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2983	The Salat Times WordPress plugin before 3.2.2 does not sanitize and escapes its settings, allowing high-privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2022-45223	Web-Based Student Clearance System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in /Admin/add-student.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the txtfullname parameter.	4.8	More Details
CVE-2022-3833	The Fancier Author Box by ThematoSoup WordPress plugin through 1.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2022-3831	The reCAPTCHA WordPress plugin through 1.6 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2022-3828	The Video Thumbnails WordPress plugin through 2.12.3 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2022-42095	Backdrop CMS version 1.23.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Page content.	4.8	More Details
CVE-2022-45221	Web-Based Student Clearance System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in changepassword.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the txtnew_password parameter.	4.8	More Details
CVE-2022-3824	The WP Admin UI Customize WordPress plugin before 1.5.13 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2022-45224	Web-Based Student Clearance System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in Admin/add-admin.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the txtfullname parameter.	4.8	More Details
CVE-2022-3834	The Google Forms WordPress plugin through 0.95 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2022-3823	The Beautiful Cookie Consent Banner WordPress plugin before 2.9.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3822	The Donations via PayPal WordPress plugin before 1.9.9 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2022-41946	pgjdbc is an open source postgresql JDBC Driver. In affected versions a prepared statement using either `PreparedStatement.setText(int, InputStream)` or `PreparedStatemet.setBytea(int, InputStream)` will create a temporary file if the InputStream is larger than 2k. This will create a temporary file which is readable by other users on Unix like systems, but not MacOS. On Unix like systems, the system's temporary directory is shared between all users on that system. Because of this, when files and directories are written into this directory they are, by default, readable by other users on that same system. This vulnerability does not allow other users to overwrite the contents of these directories or files. This is purely an information disclosure vulnerability. Because certain JDK file system APIs were only added in JDK 1.7, this this fix is dependent upon the version of the JDK you are using. Java 1.7 and higher users: this vulnerability is fixed in 4.5.0. Java 1.6 and lower users: no patch is available. If you are unable to patch, or are stuck running on Java 1.6, specifying the java.io.tmpdir system environment variable to a directory that is exclusively owned by the executing user will mitigate this vulnerability.	4.7	More Details
CVE-2022-45887	An issue was discovered in the Linux kernel through 6.0.9. drivers/media/usb/ttusb-dec/ttusb_dec.c has a memory leak because of the lack of a dvb_frontend_detach call.	4.7	More Details
CVE-2022-4029	The Simple:Press plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'sforum_[md5 hash of the WordPress URL]' cookie value in versions up to, and including, 6.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. This would be highly complex to exploit as it would require the attacker to set the cookie a cookie for the targeted user.	4.7	More Details
CVE-2022-39331	Nexcloud desktop is the Desktop sync client for Nextcloud. An attacker can inject arbitrary HyperText Markup Language into the Desktop Client application in the notifications. It is recommended that the Nextcloud Desktop client is upgraded to 3.6.1. There are no known workarounds for this issue.	4.6	More Details
CVE-2022-39332	Nexcloud desktop is the Desktop sync client for Nextcloud. An attacker can inject arbitrary HyperText Markup Language into the Desktop Client application via user status and information. It is recommended that the Nextcloud Desktop client is upgraded to 3.6.1. There are no known workarounds for this issue.	4.6	More Details
CVE-2022-39333	Nexcloud desktop is the Desktop sync client for Nextcloud. An attacker can inject arbitrary HyperText Markup Language into the Desktop Client application. It is recommended that the Nextcloud Desktop client is upgraded to 3.6.1. There are no known workarounds for this issue.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39325	BaserCMS is a content management system with a japanese language focus. In affected versions there is a cross-site scripting vulnerability on the management system of baserCMS. This is a vulnerability that needs to be addressed when the management system is used by an unspecified number of users. Users of baserCMS are advised to upgrade as soon as possible. There are no known workarounds for this vulnerability.	4.6	More Details
CVE-2020-23588	A vulnerability in OPTILINK OP-XT71000N Hardware Version: V2.2 , Firmware Version: OP_V3.3.1-191028 allows an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack to "Enable or Disable Ports" and to "Change port number" through " /rmtacc.asp ".	4.3	More Details
CVE-2022-3995	The TeraWallet plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to, and including, 1.4.3. This is due to insufficient validation of the user-controlled key on the lock_unlock_terawallet AJAX action. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to lock/unlock other users wallets.	4.3	More Details
CVE-2022-3361	The Ultimate Member plugin for WordPress is vulnerable to directory traversal in versions up to, and including 2.5.0 due to insufficient input validation on the 'template' attribute used in shortcodes. This makes it possible for attackers with administrative privileges to supply arbitrary paths using traversal (../../) to access and include files outside of the intended directory. If an attacker can successfully upload a php file then remote code execution via inclusion may also be possible. Note: for users with less than administrative capabilities, /wp-admin access needs to be enabled for that user in order for this to be exploitable by those users.	4.3	More Details
CVE-2022-46150	Discourse is an open-source discussion platform. Prior to version 2.8.13 of the `stable` branch and version 2.9.0.beta14 of the `beta` and `tests-passed` branches, unauthorized users may learn of the existence of hidden tags and that they have been applied to topics that they have access to. This issue is patched in version 2.8.13 of the `stable` branch and version 2.9.0.beta14 of the `beta` and `tests-passed` branches. As a workaround, use the `disable_email` site setting to disable all emails to non-staff users.	4.3	More Details
CVE-2020-23586	A vulnerability found in OPTILINK OP-XT71000N Hardware Version: V2.2 , Firmware Version: OP_V3.3.1-191028 allows an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack to Add Network Traffic Control Type Rule.	4.3	More Details
CVE-2021-25059	The Download Plugin WordPress plugin before 2.0.0 does not properly validate a user has the required privileges to access a backup's nonce identifier, which may allow any users with an account on the site (such as subscriber) to download a full copy of the website.	4.3	More Details
CVE-2022-4089	A vulnerability was found in rickxy Stock Management System. It has been declared as problematic. This vulnerability affects unknown code of the file /pages/processlogin.php. The manipulation of the argument user leads to cross site scripting. 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-214324.	4.3	More Details
CVE-2022-45305	Insecure permissions in Chocolatey Python3 package v3.11.0 and below grants all users in the Authenticated Users group write privileges for the subfolder C:\Python311 and all files located in that folder.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45210	Jeecg-boot v3.4.3 was discovered to contain a SQL injection vulnerability via the component /sys/user/deleteRecycleBin.	4.3	More Details
CVE-2022-4044	A denial-of-service vulnerability in Mattermost allows an authenticated user to crash the server via multiple large autoresponder messages.	4.3	More Details
CVE-2022-4019	A denial-of-service vulnerability in the Mattermost Playbooks plugin allows an authenticated user to crash the server via multiple large requests to one of the Playbooks API endpoints.	4.3	More Details
CVE-2022-3850	The Find and Replace All WordPress plugin before 1.3 does not have CSRF check when replacing string, which could allow attackers to make a logged admin replace arbitrary string in database tables via a CSRF attack	4.3	More Details
CVE-2022-45208	Jeecg-boot v3.4.3 was discovered to contain a SQL injection vulnerability via the component /sys/user/putRecycleBin.	4.3	More Details
CVE-2022-34654	Cross-Site Request Forgery (CSRF) in Virgial Berveling's Manage Notification E-mails plugin <= 1.8.2 on WordPress.	4.3	More Details
CVE-2022-4090	A vulnerability was found in rickxy Stock Management System and classified as problematic. This issue affects some unknown processing of the file us_transac.php?action=add. The manipulation leads to cross-site request forgery. 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-214331.	4.3	More Details
CVE-2022-45301	Insecure permissions in Chocolatey Ruby package v3.1.2.1 and below grants all users in the Authenticated Users group write privileges for the path C:\tools\ruby31 and all files located in that folder.	4.3	More Details
CVE-2022-45304	Insecure permissions in Chocolatey Cmder package v1.3.20 and below grants all users in the Authenticated Users group write privileges for the path C:\tools\Cmder and all files located in that folder.	4.3	More Details
CVE-2022-38377	An improper access control vulnerability [CWE-284] in FortiManager 7.2.0, 7.0.0 through 7.0.3, 6.4.0 through 6.4.7, 6.2.0 through 6.2.9, 6.0.0 through 6.0.11 and FortiAnalyzer 7.2.0, 7.0.0 through 7.0.3, 6.4.0 through 6.4.8, 6.2.0 through 6.2.10, 6.0.0 through 6.0.12 may allow a remote and authenticated admin user assigned to a specific ADOM to access other ADOMs information such as device information and dashboard information.	4.3	More Details
CVE-2022-45306	Insecure permissions in Chocolatey Azure-Pipelines-Agent package v2.211.1 and below grants all users in the Authenticated Users group write privileges for the subfolder C:\agent and all files located in that folder.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39339	user_oidc is an OpenID Connect user backend for Nextcloud. In versions prior to 1.2.1 sensitive information such as the OIDC client credentials and tokens are sent in plain text of HTTP without TLS. Any malicious actor with access to monitor user traffic may have been able to compromise account security. This issue has been addressed in in user_oidc v1.2.1. Users are advised to upgrade. Users unable to upgrade may use https to access Nextcloud. Set an HTTPS discovery URL in the provider settings (in Nextcloud OIDC admin settings).	4.3	More Details
CVE-2022-45307	Insecure permissions in Chocolatey PHP package v8.1.12 and below grants all users in the Authenticated Users group write privileges for the subfolder C:\tools\php81 and all files located in that folder.	4.3	More Details
CVE-2022-39334	Nextcloud also ships a CLI utility called nextcloudcmd which is sometimes used for automated scripting and headless servers. Versions of nextcloudcmd prior to 3.6.1 would incorrectly trust invalid TLS certificates, which may enable a Man-in-the-middle attack that exposes sensitive data or credentials to a network attacker. This affects the CLI only. It does not affect the standard GUI desktop Nextcloud clients, and it does not affect the Nextcloud server.	3.9	More Details
CVE-2022-4031	The Simple:Press plugin for WordPress is vulnerable to arbitrary file modifications in versions up to, and including, 6.8 via the 'file' parameter which does not properly restrict files to be edited in the context of the plugin. This makes it possible with attackers, with high-level permissions such as an administrator, to supply paths to arbitrary files on the server that can be modified outside of the intended scope of the plugin.	3.8	More Details
CVE-2022-29832	Cleartext Storage of Sensitive Information in Memory vulnerability in Mitsubishi Electric Corporation GX Works3 versions 1.015R and later, GX Works2 all versions and GX Developer versions 8.40S and later allows a remote unauthenticated attacker to disclose sensitive information. As a result, unauthenticated users could obtain information about the project file for MELSEC safety CPU modules or project file for MELSEC Q/FX/L series with security setting.	3.7	More Details
CVE-2022-4091	A vulnerability was found in SourceCodester Canteen Management System. It has been classified as problematic. This affects the function query of the file food.php. The manipulation of the argument product_name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-214359.	3.5	More Details
CVE-2022-41944	Discourse is an open-source discussion platform. In stable versions prior to 2.8.12 and beta or tests-passed versions prior to 2.9.0.beta.13, under certain conditions, a user can see notifications for topics they no longer have access to. If there is sensitive information in the topic title, it will therefore have been exposed. This issue is patched in stable version 2.8.12, beta version 2.9.0.beta13, and tests-passed version 2.9.0.beta13. There are no workarounds available.	3.5	More Details
CVE-2022-41921	Discourse is an open-source discussion platform. Prior to version 2.9.0.beta13, users can post chat messages of an unlimited length, which can cause a denial of service for other users when posting huge amounts of text. Users should upgrade to version 2.9.0.beta13, where a limit has been introduced. No known workarounds are available.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39338	user_oidc is an OpenID Connect user backend for Nextcloud. Versions prior to 1.2.1 did not properly validate discovery urls which may lead to a stored cross site scripting attack vector. The impact is limited due to the restrictive CSP that is applied on this endpoint. Additionally this vulnerability has only been shown to be exploitable in the Safari web browser. This issue has been addressed in version 1.2.1. Users are advised to upgrade. Users unable to upgrade should urge their users to avoid using the Safari web browser.	3.5	More Details
CVE-2022-39346	Nextcloud server is an open source personal cloud server. Affected versions of nextcloud server did not properly limit user display names which could allow a malicious users to overload the backing database and cause a denial of service. It is recommended that the Nextcloud Server is upgraded to 22.2.10, 23.0.7 or 24.0.3. There are no known workarounds for this issue.	3.5	More Details
CVE-2022-41954	MPXJ is an open source library to read and write project plans from a variety of file formats and databases. On Unix-like operating systems (not Windows or macos), MPXJ's use of `File.createTempFile(..)` results in temporary files being created with the permissions `-rw-r--r--`. This means that any other user on the system can read the contents of this file. When MPXJ is reading a schedule file which requires the creation of a temporary file or directory, a knowledgeable local user could locate these transient files while they are in use and would then be able to read the schedule being processed by MPXJ. The problem has been patched, MPXJ version 10.14.1 and later includes the necessary changes. Users unable to upgrade may set `java.io.tmpdir` to a directory to which only the user running the application has access will prevent other users from accessing these temporary files.	3.3	More Details
CVE-2022-41926	Nextcould talk android is the android OS implementation of the nextcloud talk chat system. In affected versions the receiver is not protected by broadcastPermission allowing malicious apps to monitor communication. It is recommended that the Nextcloud Talk Android is upgraded to 14.1.0. There are no known workarounds for this issue.	3.3	More Details
CVE-2020-23587	A vulnerability found in the OPTILINK OP-XT71000N Hardware Version: V2.2 , Firmware Version: OP_V3.3.1-191028 allows an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack to men in the middle attack by adding New Routes in RoutingConfiguration on " /routing.asp ".	3.1	More Details
CVE-2022-4045	A denial-of-service vulnerability in the Mattermost allows an authenticated user to crash the server via multiple requests to one of the API endpoints which could fetch a large amount of data.	3.1	More Details
CVE-2022-32967	RTL8111EP-CG/RTL8111FP-CG DASH function has hard-coded password. An unauthenticated physical attacker can use the hard-coded default password during system reboot triggered by other user, to acquire partial system information such as serial number and server information.	2.1	More Details