SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 27 April 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-2022-24861	Databasir is a team-oriented relational database model document management platform. Databasir 1.01 has remote code execution vulnerability. JDBC drivers are not validated prior to use and may be provided by users of the system. This can lead to code execution by any basic user who has access to the system. Users are advised to upgrade. There are no known workarounds to this issue.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24826	On Windows, if Git LFS operates on a malicious repository with a `..exe` file as well as a file named `git.exe`, and `git.exe` is not found in `PATH`, the `..exe` program will be executed, permitting the attacker to execute arbitrary code. This does not affect Unix systems. Similarly, if the malicious repository contains files named `..exe` and `cygpath.exe`, and `cygpath.exe` is not found in `PATH`, the `..exe` program will be executed when certain Git LFS commands are run. More generally, if the current working directory contains any file with a base name of `.` and a file extension from `PATHEXT` (except `.bat` and `.cmd`), and also contains another file with the same base name as a program Git LFS intends to execute (such as `git`, `cygpath`, or `uname`) and any file extension from `PATHEXT` (including `.bat` and `.cmd`), then, on Windows, when Git LFS attempts to execute the intended program the `..exe`, `..com`, etc., file will be executed instead, but only if the intended program is not found in any directory listed in `PATH`. The vulnerability occurs because when Git LFS detects that the program it intends to run does not exist in any directory listed in `PATH` then Git LFS passes an empty string as the executable file path to the Go `os/exec` package, which contains a bug such that, on Windows, it prepends the name of the current working directory (i.e., `.`) to the empty string without adding a path separator, and as a result searches in that directory for a file with the base name `.` combined with any file extension from `PATHEXT`, executing the first one it finds. (The reason `..bat` and `..cmd` files are not executed in the same manner is that, although the Go `os/exec` package tries to execute them just as it does a `..exe` file, the Microsoft Win32 API `CreateProcess()` family of functions have an undocumented feature in that they apparently recognize when a caller is attempting to execute a batch script file and instead run the `cmd.exe` command interpreter, passing the full set of command line arguments as parameters. These are unchanged from the command line arguments set by Git LFS, and as such, the intended program's name is the first, resulting in a command line like `cmd.exe /c git`, which then fails.) Git LFS has resolved this vulnerability by always reporting an error when a program is not found in any directory listed in `PATH` rather than passing an empty string to the Go `os/exec` package in this case. The bug in the Go `os/exec` package has been reported to the Go project and is expected to be patched after this security advisory is published. The problem was introduced in version 2.12.1 and is patched in version 3.1.3. Users of affected versions should upgrade to version 3.1.3. There are currently no known workarounds at this time.	9.8	More Details
CVE-2022-27341	JFinalCMS v2.0 was discovered to contain a SQL injection vulnerability via the Article Management function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45840	It is possible to execute arbitrary commands as root in Terramaster F4-210, F2-210 TOS 4.2.X (4.2.15-2107141517) by sending specifically crafted input to /tos/index.php?app/app_start_stop.	9.8	More Details
CVE-2021-45837	It is possible to execute arbitrary commands as root in Terramaster F4-210, F2-210 TOS 4.2.X (4.2.15-2107141517) by sending a specifically crafted input to /tos/index.php?app/del.	9.8	More Details
CVE-2022-29264	An issue was discovered in coreboot 4.13 through 4.16. On APs, arbitrary code execution in SMM may occur.	9.8	More Details
CVE-2022-29077	A heap-based buffer overflow exists in rippled before 1.8.5. The vulnerability allows attackers to cause a crash or execute commands remotely on a rippled node, which may lead to XRPL mainnet DoS or compromise. This exposes all digital assets on the XRPL to a security threat.	9.8	More Details
CVE-2021-3897	An authentication bypass vulnerability was discovered in an internal service of the Lenovo Fan Power Controller2 (FPC2) and Lenovo System Management Module (SMM) firmware during an that could allow an unauthenticated attacker to execute commands on the SMM and FPC2. SMM2 is not affected.	9.8	More Details
CVE-2021-3849	An authentication bypass vulnerability was discovered in the web interface of the Lenovo Fan Power Controller2 (FPC2) and Lenovo System Management Module (SMM) firmware that could allow an unauthenticated attacker to execute commands on the SMM and FPC2. SMM2 is not affected.	9.8	More Details
CVE-2022-27342	Link-Admin v0.0.1 was discovered to contain a SQL injection vulnerability via DictRest.ResponseResult().	9.8	More Details
CVE-2022-1440	Command Injection vulnerability in git-interface@2.1.1 in GitHub repository yarkeev/git-interface prior to 2.1.2. If both are provided by user input, then the use of a `--upload-pack` command-line argument feature of git is also supported for `git clone`, which would then allow for any operating system command to be spawned by the attacker.	9.8	More Details
CVE-2022-27429	Jizhicms v1.9.5 was discovered to contain a Server-Side Request Forgery (SSRF) vulnerability via /admin.php/Plugins/update.html.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27404	FreeType commit 1e2eb65048f75c64b68708efed6ce904c31f3b2f was discovered to contain a heap buffer overflow via the function sfnt_init_face.	9.8	More Details
CVE-2022-26674	ASUS RT-AX88U has a Format String vulnerability, which allows an unauthenticated remote attacker to write to arbitrary memory address and perform remote arbitrary code execution, arbitrary system operation or disrupt service.	9.8	More Details
CVE-2022-28439	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/uesrs.php&&action=delete&userid=4.	9.8	More Details
CVE-2022-28438	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/uesrs.php&action=type&userrole=User&userid=.	9.8	More Details
CVE-2022-28437	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/uesrs.php&action=type&userrole=Admin&userid=3.	9.8	More Details
CVE-2022-28436	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/uesrs.php&action=display&value=Hide&userid=.	9.8	More Details
CVE-2022-28435	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/siteoptions.php&action=displaygoal&value=1&roleid=1.	9.8	More Details
CVE-2022-27311	Gibbon v3.4.4 and below allows attackers to execute a Server-Side Request Forgery (SSRF) via a crafted URL.	9.8	More Details
CVE-2022-28093	SCBS Online Sports Venue Reservation System v1.0 was discovered to contain a local file inclusion vulnerability which allow attackers to execute arbitrary code via a crafted PHP file.	9.8	More Details
CVE-2022-28433	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/uesrs.php&action=display&value=Show&userid=.	9.8	More Details
CVE-2022-29806	ZoneMinder before 1.36.13 allows remote code execution via an invalid language. Ability to create a debug log file at an arbitrary pathname contributes to exploitability.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28521	ZCMS v20170206 was discovered to contain a file inclusion vulnerability via index.php?m=home&c=home&a=sp_set_config.	9.8	More Details
CVE-2022-27985	CuppaCMS v1.0 was discovered to contain a SQL injection vulnerability via /administrator/alerts/alertLightbox.php.	9.8	More Details
CVE-2022-27984	CuppaCMS v1.0 was discovered to contain a SQL injection vulnerability via the menu_filter parameter at /administrator/templates/default/html/windows/right.php.	9.8	More Details
CVE-2022-27469	Monstaftp v2.10.3 was discovered to allow attackers to execute Server-Side Request Forgery (SSRF).	9.8	More Details
CVE-2022-27468	Monstaftp v2.10.3 was discovered to contain an arbitrary file upload which allows attackers to execute arbitrary code via a crafted file uploaded to the web server.	9.8	More Details
CVE-2022-27299	Hospital Management System v1.0 was discovered to contain a SQL injection vulnerability via the component room.php.	9.8	More Details
CVE-2022-24706	In Apache CouchDB prior to 3.2.2, an attacker can access an improperly secured default installation without authenticating and gain admin privileges. The CouchDB documentation has always made recommendations for properly securing an installation, including recommending using a firewall in front of all CouchDB installations.	9.8	More Details
CVE-2022-29499	The Service Appliance component in Mitel MiVoice Connect through 19.2 SP3 allows remote code execution because of incorrect data validation. The Service Appliances are SA 100, SA 400, and Virtual SA.	9.8	More Details
CVE-2022-29078	The ejs (aka Embedded JavaScript templates) package 3.1.6 for Node.js allows server-side template injection in settings[view options][outputFunctionName]. This is parsed as an internal option, and overwrites the outputFunctionName option with an arbitrary OS command (which is executed upon template compilation).	9.8	More Details
CVE-2022-1391	The Cab fare calculator WordPress plugin before 1.0.4 does not validate the controller parameter before using it in require statements, which could lead to Local File Inclusion issues.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1390	The Admin Word Count Column WordPress plugin through 2.2 does not validate the path parameter given to readfile(), which could allow unauthenticated attackers to read arbitrary files on server running old version of PHP susceptible to the null byte technique. This could also lead to RCE by using a Phar Deserialization technique	9.8	More Details
CVE-2022-0782	The Donations WordPress plugin through 1.8 does not sanitise and escape the nd_donations_id parameter before using it in a SQL statement via the nd_donations_single_cause_form_validate_fields_php_function AJAX action (available to unauthenticated users), leading to an unauthenticated SQL Injection	9.8	More Details
CVE-2022-0769	The Users Ultra WordPress plugin through 3.1.0 fails to properly sanitize and escape the data_target parameter before it is being interpolated in an SQL statement and then executed via the rating_vote AJAX action (available to both unauthenticated and authenticated users), leading to an SQL Injection.	9.8	More Details
CVE-2022-0693	The Master Elements WordPress plugin through 8.0 does not validate and escape the meta_ids parameter of its remove_post_meta_condition AJAX action (available to both unauthenticated and authenticated users) before using it in a SQL statement, leading to an unauthenticated SQL Injection	9.8	More Details
CVE-2022-0657	The 5 Stars Rating Funnel WordPress Plugin	RRatingg WordPress plugin before 1.2.54 does not properly sanitise, validate and escape lead ids before using them in a SQL statement via the rrtngg_delete_leads AJAX action, available to unauthenticated users, leading to an unauthenticated SQL injection issue. There is an attempt to sanitise the input, using sanitize_text_field(), however such function is not intended to prevent SQL injections.	9.8	More Details
CVE-2022-0541	The flo-launch WordPress plugin before 2.4.1 injects code into wp-config.php when creating a cloned site, allowing any attacker to initiate a new site install by setting the flo_custom_table_prefix cookie to an arbitrary value.	9.8	More Details
CVE-2022-28434	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin.php?id=siteoptions&social=edit&sid=2.	9.8	More Details
CVE-2022-28432	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin.php?id=siteoptions&social=display&value=0&sid=2.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28029	Simple Real Estate Portal System v1.0 was discovered to contain a SQL injection vulnerability via /reps/classes/Master.php?f=delete_type.	9.8	More Details
CVE-2022-28411	Simple Real Estate Portal System v1.0 was discovered to contain a SQL injection vulnerability via /reps/admin/?page=agents/manage_agent.	9.8	More Details
CVE-2022-28030	Simple Real Estate Portal System v1.0 was discovered to contain a SQL injection vulnerability via /reps/classes/Master.php?f=delete_estate.	9.8	More Details
CVE-2022-28431	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/siteoptions.php&social=remove&sid=2.	9.8	More Details
CVE-2022-28028	Simple Real Estate Portal System v1.0 was discovered to contain a SQL injection vulnerability via /reps/classes/Master.php?f=delete_amenity.	9.8	More Details
CVE-2022-28026	Student Grading System v1.0 was discovered to contain a SQL injection vulnerability via /student-grading-system/rms.php?page=student_p&id=.	9.8	More Details
CVE-2022-28025	Student Grading System v1.0 was discovered to contain a SQL injection vulnerability via /student-grading-system/rms.php?page=school_year.	9.8	More Details
CVE-2022-28024	Student Grading System v1.0 was discovered to contain a SQL injection vulnerability via /student-grading-system/rms.php?page=grade.	9.8	More Details
CVE-2022-28023	Purchase Order Management System v1.0 was discovered to contain a SQL injection vulnerability via /purchase_order/classes/Master.php?f=delete_supplier.	9.8	More Details
CVE-2022-28022	Purchase Order Management System v1.0 was discovered to contain a SQL injection vulnerability via /purchase_order/classes/Master.php?f=delete_item.	9.8	More Details
CVE-2022-28021	Purchase Order Management System v1.0 was discovered to contain a remote code execution (RCE) vulnerability via /purchase_order/admin/?page=user.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0272	Improper Restriction of XML External Entity Reference in GitHub repository detekt/detekt prior to 1.20.0.	9.8	More Details
CVE-2016-20014	In pam_tacplus.c in pam_tacplus before 1.4.1, pam_sm_acct_mgmt does not zero out the arep data structure.	9.8	More Details
CVE-2022-29528	An issue was discovered in MISP before 2.4.158. PHAR deserialization can occur.	9.8	More Details
CVE-2021-43481	An SQL Injection vulnerability exists in Webtareas 2.4p3 and earlier via the $uq HTTP POST parameter in editapprovalstage.php.	9.8	More Details
CVE-2022-26133	SharedSecretClusterAuthenticator in Atlassian Bitbucket Data Center versions 5.14.0 and later before 7.6.14, 7.7.0 and later prior to 7.17.6, 7.18.0 and later prior to 7.18.4, 7.19.0 and later prior to 7.19.4, and 7.20.0 allow a remote, unauthenticated attacker to execute arbitrary code via Java deserialization.	9.8	More Details
CVE-2022-0540	A vulnerability in Jira Seraph allows a remote, unauthenticated attacker to bypass authentication by sending a specially crafted HTTP request. This affects Atlassian Jira Server and Data Center versions before 8.13.18, versions 8.14.0 and later before 8.20.6, and versions 8.21.0 and later before 8.22.0. This also affects Atlassian Jira Service Management Server and Data Center versions before 4.13.18, versions 4.14.0 and later before 4.20.6, and versions 4.21.0 and later before 4.22.0.	9.8	More Details
CVE-2022-28410	Simple Real Estate Portal System v1.0 was discovered to contain a SQL injection vulnerability via /reps/classes/Users.php?f=delete_agent.	9.8	More Details
CVE-2022-28524	ED01-CMS v20180505 was discovered to contain a SQL injection vulnerability via the component post.php.	9.8	More Details
CVE-2022-28412	Car Driving School Managment System v1.0 was discovered to contain a SQL injection vulnerability via /cdsms/classes/Master.php?f=delete_package.	9.8	More Details
CVE-2022-28422	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/posts.php&action=edit.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28429	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/inbox.php&action=delete&msgid=.	9.8	More Details
CVE-2022-28427	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/inbox.php&action=read&msgid=.	9.8	More Details
CVE-2022-28426	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/pagerole.php&action=edit&roleid=.	9.8	More Details
CVE-2022-28425	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/pagerole.php&action=display&value=1&roleid=.	9.8	More Details
CVE-2022-28424	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/posts.php&find=.	9.8	More Details
CVE-2022-28413	Car Driving School Management System v1.0 was discovered to contain a SQL injection vulnerability via /cdsms/classes/Master.php?f=delete_enrollment.	9.8	More Details
CVE-2022-28423	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/posts.php&action=delete.	9.8	More Details
CVE-2022-28421	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin.php?id=posts&action=display&value=1&postid=.	9.8	More Details
CVE-2022-28420	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via BabyCare/admin.php?id=theme&setid=.	9.8	More Details
CVE-2022-28417	Home Owners Collection Management System v1.0 was discovered to contain a SQL injection vulnerability via /hocms/classes/Master.php?f=delete_phase.	9.8	More Details
CVE-2022-28416	Home Owners Collection Management System v1.0 was discovered to contain a SQL injection vulnerability via /hocms/classes/Master.php?f=delete_phase.	9.8	More Details
CVE-2022-28415	Home Owners Collection Management System v1.0 was discovered to contain a SQL injection vulnerability via /hocms/classes/Master.php?f=delete_collection.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28414	Home Owners Collection Management System v1.0 was discovered to contain a SQL injection vulnerability via /hocms/classes/Master.php?f=delete_member.	9.8	More Details
CVE-2022-24799	wire-webapp is the web application interface for the wire messaging service. Insufficient escaping in markdown “code highlighting” in the wire-webapp resulted in the possibility of injecting and executing arbitrary HTML code and thus also JavaScript. If a user receives and views such a malicious message, arbitrary code is injected and executed in the context of the victim. This allows the attacker to fully control the user account. Wire-desktop clients that are connected to a vulnerable wire-webapp version are also vulnerable to this attack. The issue has been fixed in wire-webapp 2022-03-30-production.0 and is already deployed on all Wire managed services. On-premise instances of wire-webapp need to be updated to docker tag 2022-03-30-production.0-v0.29.2-0-d144552 or wire-server 2022-03-30 (chart/4.8.0), so that their applications are no longer affected. There are no known workarounds for this issue. ### Patches * The issue has been fixed in wire-webapp **2022-03-30-production.0** and is already deployed on all Wire managed services. * On-premise instances of wire-webapp need to be updated to docker tag **2022-03-30-production.0-v0.29.2-0-d144552** or wire-server **2022-03-30 (chart/4.8.0)**, so that their applications are no longer affected. ### Workarounds * No workarounds known ### For more information If you have any questions or comments about this advisory feel free to email us at vulnerability-report@wire.com ### Credits We thank [Posix](https://twitter.com/po6ix) for reporting this vulnerability	9.6	More Details
CVE-2022-1039	The weak password on the web user interface can be exploited via HTTP or HTTPS. Once such access has been obtained, the other passwords can be changed. The weak password on Linux accounts can be accessed via SSH or Telnet, the former of which is by default enabled on trusted interfaces. While the SSH service does not support root login, a user logging in using either of the other Linux accounts may elevate to root access using the su command if they have access to the associated password.	9.6	More Details
CVE-2021-41162	Combodo iTop is a web based IT Service Management tool. In 3.0.0 beta releases prior to beta6 the `ajax.render.php?operation=wizard_helper` page did not properly escape the user supplied parameters, allowing for a cross site scripting attack vector. Users are advised to upgrade. There are no known workarounds for this issue.	9.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41161	Combodo iTop is a web based IT Service Management tool. In versions prior to 3.0.0-beta6 the export CSV page don't properly escape the user supplied parameters, allowing for javascript injection into rendered csv files. Users are advised to upgrade. There are no known workarounds for this issue.	9.3	More Details
CVE-2022-28443	UCMS v1.6 was discovered to contain an arbitrary file deletion vulnerability.	9.1	More Details
CVE-2022-28743	Time-of-check Time-of-use (TOCTOU) Race Condition vulerability in Foscam R2C IP camera running System FW <= 1.13.1.6, and Application FW <= 2.91.2.66, allows an authenticated remote attacker with administrator permissions to execute arbitrary remote code via a malicious firmware patch. The impact of this vulnerability is that the remote attacker could gain full remote access to the IP camera and the underlying Linux system with root permissions. With root access to the camera's Linux OS, an attacker could effectively change the code that is running, add backdoor access, or invade the privacy of the user by accessing the live camera stream.	9.1	More Details
CVE-2022-24882	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP). In versions prior to 2.7.0, NT LAN Manager (NTLM) authentication does not properly abort when someone provides and empty password value. This issue affects FreeRDP based RDP Server implementations. RDP clients are not affected. The vulnerability is patched in FreeRDP 2.7.0. There are currently no known workarounds.	9.1	More Details
CVE-2022-0567	A flaw was found in ovn-kubernetes. This flaw allows a system administrator or privileged attacker to create an egress network policy that bypasses existing ingress policies of other pods in a cluster, allowing network traffic to access pods that should not be reachable. This issue results in information disclosure and other attacks on other pods that should not be reachable.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-28009	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\attendance_delete.php.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28018	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\schedule_edit.php.	8.8	More Details
CVE-2021-4225	The SP Project & Document Manager WordPress plugin before 4.24 allows any authenticated users, such as subscribers, to upload files. The plugin attempts to prevent PHP and other similar files that could be executed on the server from being uploaded by checking the file extension. It was discovered that on Windows servers, the security checks in place were insufficient, enabling bad actors to potentially upload backdoors on vulnerable sites.	8.8	More Details
CVE-2021-38886	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.1.7 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 209399.	8.8	More Details
CVE-2022-27629	Cross-site request forgery (CSRF) vulnerability in 'MicroPayments - Paid Author Subscriptions, Content, Downloads, Membership' versions prior to 1.9.6 allows a remote unauthenticated attacker to hijack the authentication of an administrator and perform unintended operation via unspecified vectors.	8.8	More Details
CVE-2021-26629	A path traversal vulnerability in XPLATFORM's runtime archive function could lead to arbitrary file creation. When the .xzip archive file is decompressed, an arbitrary file can be d in the parent path by using the path traversal pattern '..\'.	8.8	More Details
CVE-2022-28015	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\cashadvance_edit.php.	8.8	More Details
CVE-2022-24881	Ballcat Codegen provides the function of online editing code to generate templates. In versions prior to 1.0.0.beta.2, attackers can implement remote code execution through malicious code injection of the template engine. This happens because Velocity and freemarker templates are introduced but input verification is not done. The fault is rectified in version 1.0.0.beta.2.	8.8	More Details
CVE-2020-14120	Some Xiaomi models have a vulnerability in a certain application. The vulnerability is caused by the lack of checksum when using a three-party application to pass in parameters, and attackers can induce users to install a malicious app and use the vulnerability to achieve elevated privileges, making the normal services of the system affected.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28440	An arbitrary file upload vulnerability in UCMS v1.6 allows attackers to execute arbitrary code via a crafted PHP file.	8.8	More Details
CVE-2022-28020	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\position_edit.php.	8.8	More Details
CVE-2022-28019	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\employee_edit.php.	8.8	More Details
CVE-2022-28017	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\overtime_edit.php.	8.8	More Details
CVE-2022-28525	ED01-CMS v20180505 was discovered to contain an arbitrary file upload vulnerability via /admin/users.php?source=edit_user&id=1.	8.8	More Details
CVE-2022-28016	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\deduction_edit.php.	8.8	More Details
CVE-2022-27478	Victor v1.0 was discovered to contain a remote code execution (RCE) vulnerability via the component admin/profile.php?section=admin.	8.8	More Details
CVE-2022-28006	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\employee_delete.php.	8.8	More Details
CVE-2022-28007	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\cashadvance_delete.php.	8.8	More Details
CVE-2022-28008	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\attendance_delete.php.	8.8	More Details
CVE-2022-28053	Typemill v1.5.3 was discovered to contain an arbitrary file upload vulnerability via the upload function. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.	8.8	More Details
CVE-2022-28010	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\overtime_delete.php.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28011	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\schedule_delete.php.	8.8	More Details
CVE-2022-28012	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\position_delete.php.	8.8	More Details
CVE-2022-28013	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\schedule_employee_edit.php.	8.8	More Details
CVE-2022-27340	MCMS v5.2.7 contains a Cross-Site Request Forgery (CSRF) via /role/saveOrUpdateRole.do. This vulnerability allows attackers to escalate privileges and modify data.	8.8	More Details
CVE-2022-28014	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\attendance_edit.php.	8.8	More Details
CVE-2022-28528	bloofoxCMS v0.5.2.1 was discovered to contain an arbitrary file upload vulnerability via /admin/index.php?mode=content&page=media&action=edit.	8.8	More Details
CVE-2021-24957	The Advanced Page Visit Counter WordPress plugin before 6.1.6 does not escape the artID parameter before using it in a SQL statement in the apvc_reset_count_art AJAX action, available to any authenticated user, leading to a SQL injection	8.8	More Details
CVE-2022-26111	The BeanShell components of IRISNext through 9.8.28 allow execution of arbitrary commands on the target server by creating a custom search (or editing an existing/predefined search) of the documents. The search components permit adding BeanShell expressions that result in Remote Code Execution in the context of the IRISNext application user, running on the web server.	8.8	More Details
CVE-2021-45836	An authenticated attacker can execute arbitrary commands as root in Terramaster F4-210, F2-210 TOS 4.2.X (4.2.15-2107141517) by injecting a maliciously crafted input in the request through /tos/index.php?app/hand_app.	8.8	More Details
CVE-2022-24870	Combodo iTop is a web based IT Service Management tool. In 3.0.0 beta releases prior to 3.0.0 beta3 a malicious script can be injected in tooltips using iTop customization mechanism. This provides a stored cross site scripting attack vector to authorized users of the system. Users are advised to upgrade. There are no known workarounds for this issue.	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26516	Authorized users may install a maliciously modified package file when updating the device via the web user interface. The user may inadvertently use a package file obtained from an unauthorized source or a file that was compromised between download and deployment.	8.4	More Details
CVE-2022-1459	Non-Privilege User Can View Patient’s Disclosures in GitHub repository openemr/openemr prior to 6.1.0.1.	8.3	More Details
CVE-2022-26856	Dell EMC Repository Manager version 3.4.0 contains a plain-text password storage vulnerability. A local attacker could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application's database with privileges of the compromised account.	8.2	More Details
CVE-2022-25866	The package czproject/git-php before 4.0.3 are vulnerable to Command Injection via git argument injection. When calling the isRemoteUrlReadable($url, array $refs = NULL) function, both the url and refs parameters are passed to the git ls-remote subcommand in a way that additional flags can be set. The additional flags can be used to perform a command injection.	8.1	More Details
CVE-2022-29603	A SQL Injection vulnerability exists in UniverSIS UniverSIS-API through 1.2.1 via the $select parameter to multiple API endpoints. A remote authenticated attacker could send crafted SQL statements to a vulnerable endpoint (such as /api/students/me/messages/) to, for example, retrieve personal information or change grades.	8.1	More Details
CVE-2021-26628	Insufficient script validation of the admin page enables XSS, which causes unauthorized users to steal admin privileges. When uploading file in a specific menu, the verification of the files is insufficient. It allows remote attackers to upload arbitrary files disguising them as image files.	8.1	More Details
CVE-2022-28918	GreenCMS v2.3.0603 was discovered to contain an arbitrary file deletion vulnerability via /index.php?m=admin&c=custom&a=plugindelhandle&plugin_name=.	8.1	More Details
CVE-2021-40680	There is a Directory Traversal vulnerability in Artica Proxy (4.30.000000 SP206 through SP255, and VMware appliance 4.30.000000 through SP273) via the filename parameter to /cgi-bin/main.cgi.	8.1	More Details
CVE-2022-28527	dhcms v20170919 was discovered to contain an arbitrary folder deletion vulnerability via /admin.php?r=admin/AdminBackup/del.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25094	The Tatsu WordPress plugin before 3.3.12 add_custom_font action can be used without prior authentication to upload a rogue zip file which is uncompressed under the WordPress's upload directory. By adding a PHP shell with a filename starting with a dot ".", this can bypass extension control implemented in the plugin. Moreover, there is a race condition in the zip extraction process which makes the shell file live long enough on the filesystem to be callable by an attacker.	8.1	More Details
CVE-2022-29566	The Bulletproofs 2017/1066 paper mishandles Fiat-Shamir generation because the hash computation fails to include all of the public values from the Zero Knowledge proof statement as well as all of the public values computed in the proof, aka the Frozen Heart issue.	8.1	More Details
CVE-2022-28058	Verydows v2.0 was discovered to contain an arbitrary file deletion vulnerability via \backend\file_controller.php.	8.1	More Details
CVE-2021-45841	In Terramaster F4-210, F2-210 TOS 4.2.X (4.2.15-2107141517), an attacker can self-sign session cookies by knowing the target's MAC address and the user's password hash. Guest users (disabled by default) can be abused using a null/empty hash and allow an unauthenticated attacker to login as guest.	8.1	More Details
CVE-2022-25342	An issue was discovered on Olivetti d-COLOR MF3555 2XD_S000.002.271 devices. The Web Application is affected by Broken Access Control. It does not properly validate requests for access to data and functionality under the /mngset/authset path. By not verifying permissions for access to resources, it allows a potential attacker to view pages that are not allowed.	8.1	More Details
CVE-2022-28059	Verydows v2.0 was discovered to contain an arbitrary file deletion vulnerability via \backend\database_controller.php.	8.1	More Details
CVE-2022-28523	HongCMS 3.0.0 allows arbitrary file deletion via the component /admin/index.php/template/ajax?action=delete.	8.1	More Details
CVE-2022-24872	Shopware is an open commerce platform based on Symfony Framework and Vue. Permissions set to sales channel context by admin-api are still usable within normal user session. Users are advised to update to the current version 6.4.10.1. For older versions of 6.1, 6.2, and 6.3, corresponding security measures are also available via a plugin. There are no known workarounds for this issue.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39040	IBM Planning Analytics Workspace 2.0 could be vulnerable to malicious file upload by not validating the file types or sizes. Attackers can make use of this weakness and upload malicious executable files into the system and it can be sent to victim for performing further attacks. IBM X-Force ID: 214025.	8.0	More Details
CVE-2019-25059	Artifex Ghostscript through 9.26 mishandles .completefont. NOTE: this issue exists because of an incomplete fix for CVE-2019-3839.	7.8	More Details
CVE-2022-1441	MP4Box is a component of GPAC-2.0.0, which is a widely-used third-party package on RPM Fusion. When MP4Box tries to parse a MP4 file, it calls the function `diST_box_read()` to read from video. In this function, it allocates a buffer `str` with fixed length. However, content read from `bs` is controllable by user, so is the length, which causes a buffer overflow.	7.8	More Details
CVE-2021-36460	VeryFitPro (com.veryfit2hr.second) 3.2.8 hashes the account's password locally on the device and uses the hash to authenticate in all communication with the backend API, including login, registration and changing of passwords. This allows an attacker in possession of a hash to takeover a user's account, rendering the benefits of storing hashed passwords in the database useless.	7.8	More Details
CVE-2022-20732	A vulnerability in the configuration file protections of Cisco Virtualized Infrastructure Manager (VIM) could allow an authenticated, local attacker to access confidential information and elevate privileges on an affected device. This vulnerability is due to improper access permissions for certain configuration files. An attacker with low-privileged credentials could exploit this vulnerability by accessing an affected device and reading the affected configuration files. A successful exploit could allow the attacker to obtain internal database credentials, which the attacker could use to view and modify the contents of the database. The attacker could use this access to the database to elevate privileges on the affected device.	7.8	More Details
CVE-2022-22392	IBM Planning Analytics Local 2.0 could allow an attacker to upload arbitrary executable files which, when executed by an unsuspecting victim could result in code execution. IBM X-Force ID: 222066.	7.8	More Details
CVE-2022-29583	service_windows.go in the kardianos service package for Go omits quoting that is sometimes needed for execution of a Windows service executable from the intended directory. NOTE: this finding could not be reproduced by its original reporter or by others.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1427	Out-of-bounds Read in mrb_obj_is_kind_of in in GitHub repository mruby/mruby prior to 3.2. # Impact: Possible arbitrary code execution if being exploited.	7.8	More Details
CVE-2022-24862	Databasir is a team-oriented relational database model document management platform. Databasir 1.01 has Server-Side Request Forgery vulnerability. During the download verification process of a JDBC driver the corresponding JDBC driver download address will be downloaded first, but this address will return a response page with complete error information when accessing a non-existent URL. Attackers can take advantage of this feature for SSRF.	7.7	More Details
CVE-2022-23457	ESAPI (The OWASP Enterprise Security API) is a free, open source, web application security control library. Prior to version 2.3.0.0, the default implementation of `Validator.getValidDirectoryPath(String, String, File, boolean)` may incorrectly treat the tested input string as a child of the specified parent directory. This potentially could allow control-flow bypass checks to be defeated if an attack can specify the entire string representing the 'input' path. This vulnerability is patched in release 2.3.0.0 of ESAPI. As a workaround, it is possible to write one's own implementation of the Validator interface. However, maintainers do not recommend this.	7.5	More Details
CVE-2022-27406	FreeType commit 22a0cccb4d9d002f33c1ba7a4b36812c7d4f46b5 was discovered to contain a segmentation violation via the function FT_Request_Size.	7.5	More Details
CVE-2022-29266	In APache APISIX before 3.13.1, the jwt-auth plugin has a security issue that leaks the user's secret key because the error message returned from the dependency lua-resty-jwt contains sensitive information.	7.5	More Details
CVE-2022-24675	encoding/pem in Go before 1.17.9 and 1.18.x before 1.18.1 has a Decode stack overflow via a large amount of PEM data.	7.5	More Details
CVE-2022-27536	Certificate.Verify in crypto/x509 in Go 1.18.x before 1.18.1 can be caused to panic on macOS when presented with certain malformed certificates. This allows a remote TLS server to cause a TLS client to panic.	7.5	More Details
CVE-2022-28327	The generic P-256 feature in crypto/elliptic in Go before 1.17.9 and 1.18.x before 1.18.1 allows a panic via long scalar input.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45842	It is possible to obtain the first administrator's hash set up in Terramaster F4-210, F2-210 TOS 4.2.X (4.2.15-2107141517) on the system as well as other information such as MAC address, internal IP address etc. by performing a request to the /module/api.php?mobile/wapNasIPS endpoint.	7.5	More Details
CVE-2022-29534	An issue was discovered in MISP before 2.4.158. In UsersController.php, password confirmation can be bypassed via vectors involving an "Accept: application/json" header.	7.5	More Details
CVE-2022-25343	An issue was discovered on Olivetti d-COLOR MF3555 2XD_S000.002.271 devices. The Web Application is affected by Denial of Service. An unauthenticated attacker, who can send POST requests to the /download/set.cgi page by manipulating the failhtmfile variable, is able to cause interruption of the service provided by the Web Application.	7.5	More Details
CVE-2022-29536	In GNOME Epiphany before 41.4 and 42.x before 42.2, an HTML document can trigger a client buffer overflow (in ephy_string_shorten in the UI process) via a long page title. The issue occurs because the number of bytes for a UTF-8 ellipsis character is not properly considered.	7.5	More Details
CVE-2022-27924	Zimbra Collaboration (aka ZCS) 8.8.15 and 9.0 allows an unauthenticated attacker to inject arbitrary memcache commands into a targeted instance. These memcache commands becomes unescaped, causing an overwrite of arbitrary cached entries.	7.5	More Details
CVE-2021-37740	A denial of service vulnerability exists in MDT's firmware for the KNXnet/IP Secure router SCN-IP100.03 and KNX IP interface SCN-IP000.03 before v3.0.4, that allows a remote attacker to turn the device unresponsive to all requests on the KNXnet/IP Secure layer, until the device is rebooted, via a SESSION_REQUEST frame with a modified total length field.	7.5	More Details
CVE-2022-29547	The CreateRedirect extension before 2022-04-14 for MediaWiki does not properly check whether the user has permissions to edit the target page. This could lead to an unauthorised (or blocked) user being able to edit a page.	7.5	More Details
CVE-2022-29498	Blazer before 2.6.0 allows SQL Injection. In certain circumstances, an attacker could get a user to run a query they would not have normally run.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14123	There is a pointer double free vulnerability in Some MIUI Services. When a function is called, the memory pointer is copied to two function modules, and an attacker can cause the pointer to be repeatedly released through malicious operations, resulting in the affected module crashing and affecting normal functionality, and if successfully exploited the vulnerability can cause elevation of privileges.	7.5	More Details
CVE-2022-0656	The Web To Print Shop : uDraw WordPress plugin before 3.3.3 does not validate the url parameter in its udraw_convert_url_to_base64 AJAX action (available to both unauthenticated and authenticated users) before using it in the file_get_contents function and returning its content base64 encoded in the response. As a result, unauthenticated users could read arbitrary files on the web server (such as /etc/passwd, wp-config.php etc)	7.5	More Details
CVE-2022-28444	UCMS v1.6 was discovered to contain an arbitrary file read vulnerability.	7.5	More Details
CVE-2022-24867	GLPI is a Free Asset and IT Management Software package, that provides ITIL Service Desk features, licenses tracking and software auditing. When you pass the config to the javascript, some entries are filtered out. The variable ldap_pass is not filtered and when you look at the source code of the rendered page, we can see the password for the root dn. Users are advised to upgrade. There is no known workaround for this issue.	7.5	More Details
CVE-2022-24424	Dell EMC AppSync versions from 3.9 to 4.3 contain a path traversal vulnerability in AppSync server. A remote unauthenticated attacker may potentially exploit this vulnerability to gain unauthorized read access to the files stored on the server filesystem, with the privileges of the running web application.	7.5	More Details
CVE-2022-1392	The Videos sync PDF WordPress plugin through 1.7.4 does not validate the p parameter before using it in an include statement, which could lead to Local File Inclusion issues	7.5	More Details
CVE-2022-29546	HtmlUnit NekoHtml Parser before 2.61.0 suffers from a denial of service vulnerability. Crafted input associated with the parsing of Processing Instruction (PI) data leads to heap memory consumption. This is similar to CVE-2022-28366 but affects a much later version of the product.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20783	A vulnerability in the packet processing functionality of Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted H.323 traffic to an affected device. A successful exploit could allow the attacker to cause the affected device to either reboot normally or reboot into maintenance mode, which could result in a DoS condition on the device.	7.5	More Details
CVE-2022-24792	PJSIP is a free and open source multimedia communication library written in C. A denial-of-service vulnerability affects applications on a 32-bit systems that use PJSIP versions 2.12 and prior to play/read invalid WAV files. The vulnerability occurs when reading WAV file data chunks with length greater than 31-bit integers. The vulnerability does not affect 64-bit apps and should not affect apps that only plays trusted WAV files. A patch is available on the `master` branch of the `pjsip/project` GitHub repository. As a workaround, apps can reject a WAV file received from an unknown source or validate the file first.	7.5	More Details
CVE-2022-20773	A vulnerability in the key-based SSH authentication mechanism of Cisco Umbrella Virtual Appliance (VA) could allow an unauthenticated, remote attacker to impersonate a VA. This vulnerability is due to the presence of a static SSH host key. An attacker could exploit this vulnerability by performing a man-in-the-middle attack on an SSH connection to the Umbrella VA. A successful exploit could allow the attacker to learn the administrator credentials, change configurations, or reload the VA. Note: SSH is not enabled by default on the Umbrella VA.	7.5	More Details
CVE-2020-14116	An intent redirection vulnerability in the Mi Browser product. This vulnerability is caused by the Mi Browser does not verify the validity of the incoming data. Attackers can perform sensitive operations by exploiting this.	7.5	More Details
CVE-2022-28366	Certain Neko-related HTML parsers allow a denial of service via crafted Processing Instruction (PI) input that causes excessive heap memory consumption. In particular, this issue exists in HtmlUnit-Neko through 2.26, and is fixed in 2.27. This issue also exists in CyberNeko HTML through 1.9.22 (also affecting OWASP AntiSamy before 1.6.6), but 1.9.22 is the last version of CyberNeko HTML. NOTE: this may be related to CVE-2022-24839.	7.5	More Details
CVE-2022-23942	Apache Doris, prior to 1.0.0, used a hardcoded key and IV to initialize the cipher used for ldap password, which may lead to information disclosure.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1429	SQL injection in GridHelperService.php in GitHub repository pimcore/pimcore prior to 10.3.6. This vulnerability is capable of steal the data	7.5	More Details
CVE-2022-27405	FreeType commit 53dfdcd8198d2b3201a23c4bad9190519ba918db was discovered to contain a segmentation violation via the function FNT_Size_Request.	7.5	More Details
CVE-2021-35250	A researcher reported a Directory Transversal Vulnerability in Serv-U 15.3. This may allow access to files relating to the Serv-U installation and server files. This issue has been resolved in Serv-U 15.3 Hotfix 1.	7.5	More Details
CVE-2022-24860	Databasir is a team-oriented relational database model document management platform. Databasir 1.01 has Use of Hard-coded Cryptographic Key vulnerability. An attacker can use hard coding to generate login credentials of any user and log in to the service background located at different IP addresses.	7.4	More Details
CVE-2022-24883	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP). Prior to version 2.7.0, server side authentication against a `SAM` file might be successful for invalid credentials if the server has configured an invalid `SAM` file path. FreeRDP based clients are not affected. RDP server implementations using FreeRDP to authenticate against a `SAM` file are affected. Version 2.7.0 contains a fix for this issue. As a workaround, use custom authentication via `HashCallback` and/or ensure the `SAM` database path configured is valid and the application has file handles left.	7.4	More Details
CVE-2022-0354	A vulnerability was reported in Lenovo System Update that could allow a local user with interactive system access the ability to execute code with elevated privileges only during the installation of a System Update package released before 2022-02-25 that displays a command prompt window.	7.3	More Details
CVE-2022-0192	A DLL search path vulnerability was reported in Lenovo PCManager prior to version 4.0.40.2175 that could allow privilege escalation.	7.3	More Details
CVE-2022-26672	ASUS WebStorage has a hardcoded API Token in the APP source code. An unauthenticated remote attacker can use this token to establish connections with the server and carry out login attempts to general user accounts. A successful login to a general user account allows the attacker to access, modify or delete this user account information.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24868	GLPI is a Free Asset and IT Management Software package, that provides ITIL Service Desk features, licenses tracking and software auditing. In versions prior to 10.0.0 one can exploit a lack of sanitization on SVG file uploads and inject javascript into their user avatar. As a result any user viewing the avatar will be subject to a cross site scripting attack. Users of GLPI are advised to upgrade. Users unable to upgrade should disallow SVG avatars.	7.3	More Details
CVE-2022-24871	Shopware is an open commerce platform based on Symfony Framework and Vue. In affected versions an attacker can abuse the Admin SDK functionality on the server to read or update internal resources. Users are advised to update to the current version 6.4.10.1. For older versions of 6.1, 6.2, and 6.3, corresponding security measures are also available via a plugin. There are no known workarounds for this issue.	7.2	More Details
CVE-2022-27925	Zimbra Collaboration (aka ZCS) 8.8.15 and 9.0 has mboximport functionality that receives a ZIP archive and extracts files from it. An authenticated user with administrator rights has the ability to upload arbitrary files to the system, leading to directory traversal.	7.2	More Details
CVE-2022-1451	Out-of-bounds Read in r_bin_java_constant_value_attr_new function in GitHub repository radareorg/radare2 prior to 5.7.0. The bug causes the program reads data past the end 2f the intented buffer. Typically, this can allow attackers to read sensitive information from other memory locations or cause a crash. More details see [CWE-125: Out-of-bounds read] (https://cwe.mitre.org/data/definitions/125.html).	7.1	More Details
CVE-2022-1437	Heap-based Buffer Overflow in GitHub repository radareorg/radare2 prior to 5.7.0. The bug causes the program reads data past the end of the intented buffer. Typically, this can allow attackers to read sensitive information from other memory locations or cause a crash.	7.1	More Details
CVE-2022-1452	Out-of-bounds Read in r_bin_java_bootstrap_methods_attr_new function in GitHub repository radareorg/radare2 prior to 5.7.0. The bug causes the program reads data past the end 2f the intented buffer. Typically, this can allow attackers to read sensitive information from other memory locations or cause a crash. More details see [CWE-125: Out-of-bounds read] (https://cwe.mitre.org/data/definitions/125.html).	7.1	More Details
CVE-2021-32927	An attacker may be able to inject client-side JavaScript code on multiple instances within all versions of Uffizio GPS Tracker.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29582	In the Linux kernel before 5.17.3, fs/io_uring.c has a use-after-free due to a race condition in io_uring timeouts. This can be triggered by a local user who has no access to any user namespace; however, the race condition perhaps can only be exploited infrequently.	7.0	More Details
CVE-2022-29527	Amazon AWS amazon-ssm-agent before 3.1.1208.0 creates a world-writable sudoers file, which allows local attackers to inject Sudo rules and escalate privileges to root. This occurs in certain situations involving a race condition.	7.0	More Details
CVE-2021-35229	Cross-site scripting vulnerability is present in Database Performance Monitor 2022.1.7779 and previous versions when using a complex SQL query	6.8	More Details
CVE-2021-3898	Versions of Motorola Ready For and Motorola Device Help Android applications prior to 2021-04-08 do not properly verify the server certificate which could lead to the communication channel being accessible by an attacker.	6.8	More Details
CVE-2021-3971	A potential vulnerability by a driver used during older manufacturing processes on some consumer Lenovo Notebook devices that was mistakenly included in the BIOS image could allow an attacker with elevated privileges to modify firmware protection region by modifying an NVRAM variable.	6.7	More Details
CVE-2022-1108	A potential vulnerability due to improper buffer validation in the SMI handler LenovoFlashDeviceInterface in Thinkpad X1 Fold Gen 1 could be exploited by an attacker with local access and elevated privileges to execute arbitrary code.	6.7	More Details
CVE-2021-3972	A potential vulnerability by a driver used during manufacturing process on some consumer Lenovo Notebook devices' BIOS that was mistakenly not deactivated may allow an attacker with elevated privileges to modify secure boot setting by modifying an NVRAM variable.	6.7	More Details
CVE-2021-4210	A potential vulnerability in the SMI callback function used in the NVME driver in some Lenovo Desktop, ThinkStation, and ThinkEdge models may allow an attacker with local access and elevated privileges to execute arbitrary code.	6.7	More Details
CVE-2021-3970	A potential vulnerability in LenovoVariable SMI Handler due to insufficient validation in some Lenovo Notebook models BIOS may allow an attacker with local access and elevated privileges to execute arbitrary code.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4211	A potential vulnerability in the SMI callback function used in the SMBIOS event log driver in some Lenovo Desktop, ThinkStation, and ThinkEdge models may allow an attacker with local access and elevated privileges to execute arbitrary code.	6.7	More Details
CVE-2022-1107	During an internal product security audit a potential vulnerability due to use of Boot Services in the SmmOEMInt15 SMI handler was discovered in some ThinkPad models could be exploited by an attacker with elevated privileges that could allow for execution of code.	6.7	More Details
CVE-2021-4212	A potential vulnerability in the SMI callback function used in the Legacy BIOS mode driver in some Lenovo Notebook models may allow an attacker with local access and elevated privileges to execute arbitrary code.	6.7	More Details
CVE-2022-22969	<Issue Description> Spring Security OAuth versions 2.5.x prior to 2.5.2 and older unsupported versions are susceptible to a Denial-of-Service (DoS) attack via the initiation of the Authorization Request in an OAuth 2.0 Client application. A malicious user or attacker can send multiple requests initiating the Authorization Request for the Authorization Code Grant, which has the potential of exhausting system resources using a single session. This vulnerability exposes OAuth 2.0 Client applications only.	6.5	More Details
CVE-2021-23055	On version 2.x before 2.0.3 and 1.x before 1.12.3, the command line restriction that controls snippet use with NGINX Ingress Controller does not apply to Ingress objects. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.5	More Details
CVE-2022-27374	Tenda AX12 V22.03.01.21_CN was discovered to contain a Cross-Site Request Forgery (CSRF) via the function sub_42E328 at /goform/SysToolReboot.	6.5	More Details
CVE-2022-24272	An authenticated user may trigger an invariant assertion during command dispatch due to incorrect validation on the $external database. This may result in mongod denial of service or server crash. This issue affects: MongoDB Inc. MongoDB Server v5.0 versions, prior to and including v5.0.6.	6.5	More Details
CVE-2021-20464	IBM Cognos Analytics PowerPlay (IBM Cognos Analytics 11.1.7, 11.2.0, and 11.1.7) could be vulnerable to an XML Bomb attack by a malicious authenticated user. IBM X-Force ID: 196813.	6.5	More Details
CVE-2022-27375	Tenda AX12 V22.03.01.21_CN was discovered to contain a Cross-Site Request Forgery (CSRF) via the function sub_422168 at /goform/WifiExtraSet.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1466	Due to improper authorization, Red Hat Single Sign-On is vulnerable to users performing actions that they should not be allowed to perform. It was possible to add users to the master realm even though no respective permission was granted.	6.5	More Details
CVE-2022-20790	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to read arbitrary files from the underlying operating system. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to an affected system. A successful exploit could allow the attacker to access sensitive files on the underlying operating system.	6.5	More Details
CVE-2021-38904	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.1.7 could allow a remote attacker to obtain credentials from a user's browser via incorrect autocomplete settings. IBM X-Force ID: 209693.	6.5	More Details
CVE-2022-24865	HumHub is an Open Source Enterprise Social Network. In affected versions users who are forced to change their password by an administrator may retrieve other users' data. This issue has been resolved by commit `eb83de20`. It is recommended that the HumHub is upgraded to 1.11.0, 1.10.4 or 1.9.4. There are no known workarounds for this issue.	6.5	More Details
CVE-2022-28445	KiteCMS v1.1.1 was discovered to contain an arbitrary file read vulnerability via the background management module.	6.5	More Details
CVE-2021-45839	It is possible to obtain the first administrator's hash set up on the system in Terramaster F4-210, F2-210 TOS 4.2.X (4.2.15-2107141517) as well as other information such as MAC address, internal IP address etc. by performing a request to the /module/api.php?mobile/webNasIPS endpoint.	6.5	More Details
CVE-2022-1461	Non Privilege User can Enable or Disable Registered in GitHub repository openemr/openemr prior to 6.1.0.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1318	Hills ComNav version 3002-19 suffers from a weak communication channel. Traffic across the local network for the configuration pages can be viewed by a malicious actor. The size of certain communications packets are predictable. This would allow an attacker to learn the state of the system if they can observe the traffic. This would be possible even if the traffic were encrypted, e.g., using WPA2, as the packet sizes would remain observable. The communication encryption scheme is theoretically sound, but is not strong enough for the level of protection required.	6.2	More Details
CVE-2022-26564	HotelDruid Hotel Management Software v3.0.3 contains a cross-site scripting (XSS) vulnerability via the prezzoperiodo4 parameter in creaprezzi.php.	6.1	More Details
CVE-2022-1254	A URL redirection vulnerability in Skyhigh SWG in main releases 10.x prior to 10.2.9, 9.x prior to 9.2.20, 8.x prior to 8.2.27, and 7.x prior to 7.8.2.31, and controlled release 11.x prior to 11.1.3 allows a remote attacker to redirect a user to a malicious website controlled by the attacker. This is possible because SWG incorrectly creates a HTTP redirect response when a user clicks a carefully constructed URL. Following the redirect response, the new request is still filtered by the SWG policy.	6.1	More Details
CVE-2022-28449	nopCommerce 4.50.1 is vulnerable to Cross Site Scripting (XSS). At Apply for vendor account feature, an attacker can upload an arbitrary file to the system.	6.1	More Details
CVE-2021-25111	The English WordPress Admin WordPress plugin before 1.5.2 does not validate the admin_custom_language_return_url before redirecting users o it, leading to an open redirect issue	6.1	More Details
CVE-2022-25344	An XSS issue was discovered on Olivetti d-COLOR MF3555 2XD_S000.002.271 devices. The Web Application doesn't properly check parameters, sent in a /dvcset/sysset/set.cgi POST request via the arg01.Hostname field, before saving them on the server. In addition, the JavaScript malicious content is then reflected back to the end user and executed by the web browser.	6.1	More Details
CVE-2021-43933	The affected product is vulnerable to a network-based attack by threat actors sending unimpeded requests to the receiving server, which could cause a denial-of-service condition due to lack of heap memory resources.	6.1	More Details
CVE-2022-28586	XSS in edit page of Hoosk 1.8.0 allows attacker to execute javascript code in user browser via edit page with XSS payload bypass filter some special chars.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28094	SCBS Online Sports Venue Reservation System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the fid parameter at booking.php.	6.1	More Details
CVE-2021-43988	The affected product is vulnerable to a network-based attack by threat actors utilizing crafted naming conventions of files to gain unauthorized access rights.	6.1	More Details
CVE-2021-43990	The affected product is vulnerable to a network-based attack by threat actors supplying a crafted, malicious XML payload designed to trigger an external entity reference call.	6.1	More Details
CVE-2022-28820	ACS Commons version 5.1.x (and earlier) suffers from a Reflected Cross-site Scripting (XSS) vulnerability in /apps/acs-commons/content/page-compare.html endpoint via the a and b GET parameters. User input submitted via these parameters is not validated or sanitised. An attacker must provide a link to someone with access to AEM Author, and could potentially exploit this vulnerability to inject malicious JavaScript content into vulnerable form fields and execute it within the context of the victim's browser. The exploitation of this issue requires user interaction in order to be successful.	6.1	More Details
CVE-2022-29589	Crypt Server before 3.3.0 allows XSS in the index view. This is related to serial, computername, and username.	6.1	More Details
CVE-2022-29533	An issue was discovered in MISP before 2.4.158. There is XSS in app/Controller/OrganisationsController.php in a situation with a "weird single checkbox page."	6.1	More Details
CVE-2022-0953	The Anti-Malware Security and Brute-Force Firewall WordPress plugin before 4.20.96 does not sanitise and escape the QUERY_STRING before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting in browsers which do not encode characters	6.1	More Details
CVE-2022-26596	Cross-site scripting (XSS) vulnerability in Journal module's web content display configuration page in Liferay Portal 7.1.0 through 7.3.3, and Liferay DXP 7.0 before fix pack 94, 7.1 before fix pack 19, and 7.2 before fix pack 8, allows remote attackers to inject arbitrary web script or HTML via web content template names.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20788	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified CM Session Management Edition (Unified CM SME), and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.	6.1	More Details
CVE-2022-20778	A vulnerability in the authentication component of Cisco Webex Meetings could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface. This vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the authentication component of Cisco Webex Meetings. An attacker could exploit this vulnerability by persuading a user of the interface to click a maliciously crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	6.1	More Details
CVE-2022-28290	Reflective Cross-Site Scripting vulnerability in WordPress Country Selector Plugin Version 1.6.5. The XSS payload executes whenever the user tries to access the country selector page with the specified payload as a part of the HTTP request	6.1	More Details
CVE-2022-28367	OWASP AntiSamy before 1.6.6 allows XSS via HTML tag smuggling on STYLE content with crafted input. The output serializer does not properly encode the supposed Cascading Style Sheets (CSS) content.	6.1	More Details
CVE-2021-46780	The Easy Google Maps WordPress plugin before 1.9.32 does not escape the tab parameter before outputting it back in an attribute in the admin dashboard, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2020-14118	An intent redirection vulnerability in the Mi App Store product. This vulnerability is caused by the Mi App Store does not verify the validity of the incoming data, can cause the app store to automatically download and install apps.	6.1	More Details
CVE-2022-29577	OWASP AntiSamy before 1.6.7 allows XSS via HTML tag smuggling on STYLE content with crafted input. The output serializer does not properly encode the supposed Cascading Style Sheets (CSS) content. NOTE: this issue exists because of an incomplete fix for CVE-2022-28367.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27237	There is a cross-site scripting (XSS) vulnerability in an NI Web Server component installed with several NI products. Depending on the product(s) in use, remediation guidance includes: install SystemLink version 2021 R3 or later, install FlexLogger 2022 Q2 or later, install LabVIEW 2021 SP1, install G Web Development 2022 R1 or later, or install Static Test Software Suite version 1.2 or later.	6.1	More Details
CVE-2022-27926	A reflected cross-site scripting (XSS) vulnerability in the /public/launchNewWindow.jsp component of Zimbra Collaboration (aka ZCS) 9.0 allows unauthenticated attackers to execute arbitrary web script or HTML via request parameters.	6.1	More Details
CVE-2021-46782	The Pricing Table by Supsystic WordPress plugin before 1.9.5 does not escape the tab parameter before outputting it back in an attribute in the admin dashboard, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2021-46781	The Coming Soon by Supsystic WordPress plugin before 1.7.6 does not sanitise and escape the tab parameter before outputting it back in an attribute in the admin dashboard, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-1439	Reflected XSS on demo.microweber.org/demo/module/ in GitHub repository microweber/microweber prior to 1.2.15. Execute Arbitrary JavaScript as the attacked user. It's the only payload I found working, you might need to press "tab" but there is probably a paylaod that runs without user interaction.	6.1	More Details
CVE-2022-26597	Cross-site scripting (XSS) vulnerability in the Layout module's Open Graph integration in Liferay Portal 7.3.0 through 7.4.0, and Liferay DXP 7.3 before service pack 3 allows remote attackers to inject arbitrary web script or HTML via the site name.	6.1	More Details
CVE-2022-27103	element-plus 2.0.5 is vulnerable to Cross Site Scripting (XSS) via el-table-column.	6.1	More Details
CVE-2022-29419	SQL Injection (SQLi) vulnerability in Don Crowther's 3xSocializer plugin <= 0.98.22 at WordPress possible for users with a low role like a subscriber or higher.	6.0	More Details
CVE-2021-43986	The setup program for the affected product configures its files and folders with full access, which may allow unauthorized users permission to replace original binaries and achieve privilege escalation.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38483	The affected product is vulnerable to misconfigured binaries, allowing users on the target PC with SYSTEM level privileges access to overwrite the binary and modify files to gain privilege escalation.	6.0	More Details
CVE-2022-20795	A vulnerability in the implementation of the Datagram TLS (DTLS) protocol in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause high CPU utilization, resulting in a denial of service (DoS) condition. This vulnerability is due to suboptimal processing that occurs when establishing a DTLS tunnel as part of an AnyConnect SSL VPN connection. An attacker could exploit this vulnerability by sending a steady stream of crafted DTLS traffic to an affected device. A successful exploit could allow the attacker to exhaust resources on the affected VPN headend device. This could cause existing DTLS tunnels to stop passing traffic and prevent new DTLS tunnels from establishing, resulting in a DoS condition. Note: When the attack traffic stops, the device recovers gracefully.	5.8	More Details
CVE-2022-20787	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM) Software and Cisco Unified CM Session Management Edition (SME) Software could allow an authenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected device. This vulnerability is due to insufficient CSRF protections for the web-based management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user.	5.7	More Details
CVE-2022-22558	Dell PowerEdge Server BIOS and Dell Precision Workstation 7910 and 7920 Rack BIOS contain an Improper SMM communication buffer verification vulnerability. A Local High Privileged attacker could potentially exploit this vulnerability leading to arbitrary writes or denial of service.	5.7	More Details
CVE-2022-28218	An issue was discovered in CipherMail Webmail Messenger 1.1.1 through 4.1.4. A local attacker could access secret keys (found in a Roundcube configuration file) that are used to protect Webmail user passwords and two-factor authentication (2FA).	5.5	More Details
CVE-2022-28506	There is a heap-buffer-overflow in GIFLIB 5.2.1 function DumpScreen2RGB() in gif2rgb.c:298:45.	5.5	More Details
CVE-2022-27888	Foundry Issues service versions 2.244.0 to 2.249.0 was found to be logging in a manner that captured sensitive information (session tokens). This issue was fixed in 2.249.1.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1444	heap-use-after-free in GitHub repository radareorg/radare2 prior to 5.7.0. This vulnerability is capable of inducing denial of service.	5.5	More Details
CVE-2020-14122	Some Xiaomi phones have information leakage vulnerabilities, and some of them may be able to forge a specific identity due to the lack of parameter verification, resulting in user information leakage.	5.5	More Details
CVE-2021-3721	A denial of service vulnerability was reported in Lenovo PCManager prior to version 4.0.20.10282 that could allow an attacker with local access to trigger a blue screen error.	5.5	More Details
CVE-2020-14121	A business logic vulnerability exists in Mi App Store. The vulnerability is caused by incomplete permission checks of the products being bypassed, and an attacker can exploit the vulnerability to perform a local silent installation.	5.5	More Details
CVE-2022-1420	Use of Out-of-range Pointer Offset in GitHub repository vim/vim prior to 8.2.4774.	5.5	More Details
CVE-2022-29537	gp_rtp_builder_do_hevc in ietf/rtp_pck_mpeg4.c in GPAC 2.0.0 has a heap-based buffer over-read, as demonstrated by MP4Box.	5.5	More Details
CVE-2022-27135	xpdf 4.03 has heap buffer overflow in the function readXRefTable located in XRef.cc. An attacker can exploit this bug to cause a Denial of Service (Segmentation fault) or other unspecified effects by sending a crafted PDF file to the pdftoppm binary.	5.5	More Details
CVE-2021-43708	The Labeling tool in Titus Classification Suite 18.8.1910.140 allows users to avoid the generation of a classification label by using Excel's safe mode.	5.5	More Details
CVE-2022-26519	There is no limit to the number of attempts to authenticate for the local configuration pages for the Hills ComNav Version 3002-19 interface, which allows local attackers to brute-force credentials.	5.5	More Details
CVE-2022-27854	Stored Cross-Site Scripting (XSS) vulnerability in Alexander Ustimenko's Psychological tests & quizzes plugin <= 0.21.19 on WordPress possible for users with contributor or higher role via &wpt_test_page_submit_button_caption parameter.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26673	ASUS RT-AX88U has insufficient filtering for special characters in the HTTP header parameter. A remote attacker with general user privilege can exploit this vulnerability to inject JavaScript and perform Stored Cross-Site Scripting (XSS) attacks.	5.4	More Details
CVE-2022-20786	A vulnerability in the web-based management interface of Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability is due to improper validation of user-submitted parameters. An attacker could exploit this vulnerability by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain data or modify data that is stored in the underlying database of the affected system.	5.4	More Details
CVE-2022-1173	stored xss in GitHub repository getgrav/grav prior to 1.7.33.	5.4	More Details
CVE-2022-1152	The Menubar WordPress plugin before 5.8 does not sanitise and escape the command parameter before outputting it back in the response via the menubar AJAX action (available to any authenticated users), leading to a Reflected Cross-Site Scripting	5.4	More Details
CVE-2022-22436	IBM Maximo Asset Management 7.6.1.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 224164.	5.4	More Details
CVE-2022-28448	nopCommerce 4.50.1 is vulnerable to Cross Site Scripting (XSS). An attacker (role customer) can inject javascript code to First name or Last name at Customer Info.	5.4	More Details
CVE-2022-22435	IBM Maximo Asset Management 7.6.1.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	5.4	More Details
CVE-2022-27428	A stored cross-site scripting (XSS) vulnerability in /index.php/album/add of GalleryCMS v2.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the album_name parameter.	5.4	More Details
CVE-2022-1022	Cross-site Scripting (XSS) - Stored in GitHub repository chatwoot/chatwoot prior to 2.5.0.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0398	The ThirstyAffiliates Affiliate Link Manager WordPress plugin before 3.10.5 does not have authorisation and CSRF checks when creating affiliate links, which could allow any authenticated user, such as subscriber to create arbitrary affiliate links, which could then be used to redirect users to an arbitrary website	5.4	More Details
CVE-2021-38946	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.1.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 211240.	5.4	More Details
CVE-2022-1458	Stored XSS Leads To Session Hijacking in GitHub repository openemr/openemr prior to 6.1.0.1.	5.4	More Details
CVE-2022-1457	Store XSS in title parameter executing at EditUser Page & EditProducto page in GitHub repository neorazorx/facturascripts prior to 2022.04. Cross-site scripting attacks can have devastating consequences. Code injected into a vulnerable application can exfiltrate data or install malware on the user's machine. Attackers can masquerade as authorized users via session cookies, allowing them to perform any action allowed by the user account.	5.4	More Details
CVE-2021-36867	Stored Cross-Site Scripting (XSS) vulnerability in Alexander Ustimenko's Psychological tests & quizzes plugin <= 0.21.19 on WordPress possible for users with contributor or higher user rights.	5.4	More Details
CVE-2022-29529	An issue was discovered in MISP before 2.4.158. There is stored XSS via the LinOTP login field.	5.4	More Details
CVE-2022-29530	An issue was discovered in MISP before 2.4.158. There is stored XSS in the galaxy clusters.	5.4	More Details
CVE-2022-1445	Stored Cross Site Scripting vulnerability in the checked_out_to parameter in GitHub repository snipe/snipe-it prior to 5.4.3. The vulnerability is capable of stolen the user Cookie.	5.4	More Details
CVE-2022-28522	ZCMS v20170206 was discovered to contain a stored cross-site scripting (XSS) vulnerability via index.php?m=home&c=message&a=add.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38903	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.1.7 is vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability to inject malicious script into a Web page which would be executed in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials. IBM X-Force ID: 209691.	5.4	More Details
CVE-2022-28450	nopCommerce 4.50.1 is vulnerable to Cross Site Scripting (XSS) via the "Text" parameter (forums) when creating a new post, which allows a remote attacker to execute arbitrary JavaScript code at client browser.	5.4	More Details
CVE-2022-29531	An issue was discovered in MISP before 2.4.158. There is stored XSS in the event graph via a tag name.	5.4	More Details
CVE-2020-14117	A improper permission configuration vulnerability in Xiaomi Content Center APP. This vulnerability is caused by the lack of correct permission verification in the Xiaomi content center APP, and attackers can use this vulnerability to invoke the sensitive component functions of the Xiaomi content center APP.	5.3	More Details
CVE-2022-24880	flask-session-captcha is a package which allows users to extend Flask by adding an image based captcha stored in a server side session. In versions prior to 1.2.1, he `captcha.validate()` function would return `None` if passed no value (e.g. by submitting an having an empty form). If implementing users were checking the return value to be **False**, the captcha verification check could be bypassed. Version 1.2.1 fixes the issue. Users can workaround the issue by not explicitly checking that the value is False. Checking the return value less explicitly should still work.	5.3	More Details
CVE-2021-36203	The affected product may allow an attacker to identify and forge requests to internal systems by way of a specially crafted request.	5.3	More Details
CVE-2022-24423	Dell iDRAC8 versions prior to 2.83.83.83 contain a denial of service vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability to cause resource exhaustion in the webserver, resulting in a denial of service condition.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23711	A vulnerability in Kibana could expose sensitive information related to Elastic Stack monitoring in the Kibana page source. Elastic Stack monitoring features provide a way to keep a pulse on the health and performance of your Elasticsearch cluster. Authentication with a vulnerable Kibana instance is not required to view the exposed information. The Elastic Stack monitoring exposure only impacts users that have set any of the optional monitoring.ui.elasticsearch.* settings in order to configure Kibana as a remote UI for Elastic Stack Monitoring. The same vulnerability in Kibana could expose other non-sensitive application-internal information in the page source.	5.3	More Details
CVE-2022-20804	A vulnerability in the Cisco Discovery Protocol of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an unauthenticated, adjacent attacker to cause a kernel panic on an affected system, resulting in a denial of service (DoS) condition. This vulnerability is due to incorrect processing of certain Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by continuously sending certain Cisco Discovery Protocol packets to an affected device. A successful exploit could allow the attacker to cause a kernel panic on the system that is running the affected software, resulting in a DoS condition.	5.3	More Details
CVE-2022-24875	The CVEProject/cve-services is an open source project used to operate the CVE services api. In versions up to and including 1.1.1 the `org.conroller.js` code would erroneously log user secrets. This has been resolved in commit `46d98f2b` and should be available in subsequent versions of the software. Users of the software are advised to manually apply the `46d98f2b` commit or to update when a new version becomes available. As a workaround users should inspect their logs and remove logged secrets as appropriate.	5.3	More Details
CVE-2021-3722	A denial of service vulnerability was reported in Lenovo PCManager prior to version 4.0.40.2175 that could allow configuration files to be written to non-standard locations during installation.	5.0	More Details
CVE-2022-0636	A denial of service vulnerability was reported in Lenovo Thin Installer prior to version 1.3.0039 that could trigger a system crash.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0477	An issue has been discovered in GitLab affecting all versions starting from 11.9 before 14.5.4, all versions starting from 14.6.0 before 14.6.4, all versions starting from 14.7.0 before 14.7.1. GitLab was not correctly handling bulk requests to delete existing packages from the package registries which could result in a Denial of Service under specific conditions.	4.9	More Details
CVE-2022-20789	A vulnerability in the software upgrade process of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to write arbitrary files on the affected system. This vulnerability is due to improper restrictions applied to a system script. An attacker could exploit this vulnerability by using crafted variables during the execution of a system upgrade. A successful exploit could allow the attacker to overwrite or append arbitrary data to system files using root-level privileges.	4.9	More Details
CVE-2022-29418	Authenticated (admin user role) Persistent Cross-Site Scripting (XSS) in Mark Daniels Night Mode plugin <= 1.0.0 on WordPress via vulnerable parameters: &ntmode_page_setting[enable-me], &ntmode_page_setting[bg-color], &ntmode_page_setting[txt-color], &ntmode_page_setting[anc_color].	4.8	More Details
CVE-2022-1156	The Books & Papers WordPress plugin through 0.20210223 does not escape its Custom DB prefix settings, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-1396	The Donorbox WordPress plugin before 7.1.7 does not sanitise and escape its Campaign URL settings before outputting it in an attribute, leading to a Stored Cross-Site Scripting issue even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-28074	Halo-1.5.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability via \admin\index.html#/system/tools.	4.8	More Details
CVE-2022-1228	The Opensea WordPress plugin before 1.0.3 does not sanitize and escape some of its settings, like its "Referer address" field, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2022-1153	The LayerSlider WordPress plugin before 7.1.2 does not sanitise and escape Project's slug before outputting it back in various place, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1094	The amr users WordPress plugin before 4.59.4 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	4.8	More Details
CVE-2022-1027	The Page Restriction WordPress (WP) WordPress plugin before 1.2.7 allows bad actors with administrator privileges to the settings page to inject Javascript code to its settings leading to stored Cross-Site Scripting that will only affect administrator users.	4.8	More Details
CVE-2022-0876	The Social comments by WpDevArt WordPress plugin before 2.5.0 does not sanitise and escape its settings, allowing high privilege users such as admin to perform cross-Site Scripting attacks even when unfiltered_html is disallowed	4.8	More Details
CVE-2022-29532	An issue was discovered in MISP before 2.4.158. There is XSS in the cerebrate view if one administrator puts a javascript: URL in the URL field, and another administrator clicks on it.	4.8	More Details
CVE-2021-36895	Unauthenticated Cross-Site Scripting (XSS) vulnerability in Tripetto's Tripetto plugin <= 5.1.4 on WordPress via SVG image upload.	4.7	More Details
CVE-2022-29548	A reflected XSS issue exists in the Management Console of several WSO2 products. This affects API Manager 2.2.0, 2.5.0, 2.6.0, 3.0.0, 3.1.0, 3.2.0, and 4.0.0; API Manager Analytics 2.2.0, 2.5.0, and 2.6.0; API Microgateway 2.2.0; Data Analytics Server 3.2.0; Enterprise Integrator 6.2.0, 6.3.0, 6.4.0, 6.5.0, and 6.6.0; IS as Key Manager 5.5.0, 5.6.0, 5.7.0, 5.9.0, and 5.10.0; Identity Server 5.5.0, 5.6.0, 5.7.0, 5.9.0, 5.10.0, and 5.11.0; Identity Server Analytics 5.5.0 and 5.6.0; and WSO2 Micro Integrator 1.0.0.	4.6	More Details
CVE-2022-24869	GLPI is a Free Asset and IT Management Software package, that provides ITIL Service Desk features, licenses tracking and software auditing. In versions prior to 10.0.0 one can use ticket's followups or setup login messages with a stylesheet link. This may allow for a cross site scripting attack vector. This issue is partially mitigated by cors security of browsers, though users are still advised to upgrade.	4.6	More Details
CVE-2022-27179	A malicious actor having access to the exported configuration file may obtain the stored credentials and thereby gain access to the protected resource. If the same passwords were used for other resources, further such assets may be compromised.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24866	Discourse Assign is a plugin for assigning users to a topic in Discourse, an open-source messaging platform. Prior to version 1.0.1, the UserBookmarkSerializer serialized the whole User / Group object, which leaked some private information. The data was only being serialized to people who could view assignment info, which is limited to staff by default. For the vast majority of sites, this data was only leaked to trusted staff member, but for sites with assign features enabled publicly, the data was accessible to more people than just staff. Version 1.0.1 contains a patch. There are currently no known workarounds.	4.3	More Details
CVE-2021-29824	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.1.7 is vulnerable to priviledge escalation where a lower level user could have read access to to the 'Data Connections' page to which they don't have access. IBM X-Force ID: 204468.	4.3	More Details
CVE-2022-29417	Plugin Settings Update vulnerability in ShortPixel's ShortPixel Adaptive Images plugin <= 3.3.1 at WordPress allows an attacker with a low user role like a subscriber or higher to change the plugin settings.	4.3	More Details
CVE-2022-1092	The myCred WordPress plugin before 2.4.3.1 does not have authorisation and CSRF checks in its mycred-tools-import-export AJAX action, allowing any authenticated user to call and and retrieve the list of email address present in the blog	4.3	More Details
CVE-2021-32929	All versions of Uffizio GPS Tracker may allow an attacker to perform unintended actions on behalf of a user.	4.3	More Details
CVE-2022-0634	The ThirstyAffiliates WordPress plugin before 3.10.5 lacks authorization checks in the ta_insert_external_image action, allowing a low-privilege user (with a role as low as Subscriber) to add an image from an external URL to an affiliate link. Further the plugin lacks csrf checks, allowing an attacker to trick a logged in user to perform the action by crafting a special request.	4.3	More Details
CVE-2022-0363	The myCred WordPress plugin before 2.4.3.1 does not have any authorisation and CSRF checks in the mycred-tools-import-export AJAX action, allowing any authenticated users, such as subscribers, to call it and import mycred setup, thus creating badges, managing points or creating arbitrary posts.	4.3	More Details
CVE-2022-0287	The myCred WordPress plugin before 2.4.4.1 does not have any authorisation in place in its mycred-tools-select-user AJAX action, allowing any authenticated user, such as subscriber to call and retrieve all email addresses from the blog	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38905	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.1.7 could allow an authenticated user to view report pages that they should not have access to. IBM X-Force ID: 209697.	4.3	More Details
CVE-2021-24805	The DW Question & Answer Pro WordPress plugin through 1.3.4 does not properly check for CSRF in some of its functions, allowing attackers to make logged in users perform unwanted actions, such as update a comment or a question status.	4.3	More Details
CVE-2021-24800	The DW Question & Answer Pro WordPress plugin through 1.3.4 does not check that the comment to edit belongs to the user making the request, allowing any user to edit other comments.	4.3	More Details
CVE-2022-28871	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the fsicapd component used in certain F-Secure products while scanning larger packages/fuzzed files consume too much memory eventually can crash the scanning engine. The exploit can be triggered remotely by an attacker.	4.3	More Details
CVE-2022-24864	Origin Protocol is a blockchain based project. The Origin Protocol project website allows for malicious users to inject malicious Javascript via a POST request to `/presale/join`. User-controlled data is passed with no sanitization to SendGrid and injected into an email that is delivered to the founders@originprotocol.com. If the email recipient is using an email program that is susceptible to XSS, then that email recipient will receive an email that may contain malicious XSS. Regardless if the email recipient's mail program has vulnerabilities or not, the hacker can at the very least inject malicious HTML that modifies the body content of the email. There are currently no known workarounds.	4.1	More Details
CVE-2022-20805	A vulnerability in the automatic decryption process in Cisco Umbrella Secure Web Gateway (SWG) could allow an authenticated, adjacent attacker to bypass the SSL decryption and content filtering policies on an affected system. This vulnerability is due to how the decryption function uses the TLS Sever Name Indication (SNI) extension of an HTTP request to discover the destination domain and determine if the request needs to be decrypted. An attacker could exploit this vulnerability by sending a crafted request over TLS from a client to an unknown or controlled URL. A successful exploit could allow an attacker to bypass the decryption process of Cisco Umbrella SWG and allow malicious content to be downloaded to a host on a protected network. There are workarounds that address this vulnerability.	4.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29280	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-28366. Reason: This candidate is a reservation duplicate of CVE-2022-28366. Notes: All CVE users should reference CVE-2022-28366 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2022-24874	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-28820. Reason: This candidate is a reservation duplicate of CVE-2022-28820. Notes: All CVE users should reference CVE-2022-28820 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-36628	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-40680. Reason: This candidate is a reservation duplicate of CVE-2021-40680. Notes: All CVE users should reference CVE-2021-40680 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details