SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 23 November 2022

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-42497	Arbitrary Code Execution vulnerability in Api2Cart Bridge Connector plugin <= 1.1.0 on WordPress.	10.0	More Details
CVE-2022-36786	DLINK - DSL-224 Post-auth RCE. DLINK router version 3.0.8 has an interface where you can configure NTP servers (Network Time Protocol) via jsonrpc API. It is possible to inject a command through this interface that will run with ROOT permissions on the router.	9.9	More Details
CVE-2022-40200	Auth. (subscriber+) Arbitrary File Upload vulnerability in wpForo Forum plugin <= 2.0.9 on WordPress.	9.9	More Details
CVE-2022-34827	Carel Boss Mini 1.5.0 has Improper Access Control.	9.9	More Details
CVE-2022-36227	In libarchive before 3.6.2, the software does not check for an error after calling calloc function that can return with a NULL pointer if the function fails, which leads to a resultant NULL pointer dereference. NOTE: the discoverer cites this CWE-476 remark but third parties dispute the code-execution impact: "In rare circumstances, when NULL is equivalent to the 0x0 memory address and privileged code can access it, then writing or reading memory is possible, which may lead to code execution."	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44187	Netgear R7000P V1.3.0.8 is vulnerable to Buffer Overflow via wan_dns1_pri.	9.8	More Details
CVE-2022-44186	Netgear R7000P V1.3.1.64 is vulnerable to Buffer Overflow in /usr/sbin/httpd via parameter wan_dns1_pri.	9.8	More Details
CVE-2022-40189	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Apache Airflow Pig Provider, Apache Airflow allows an attacker to control commands executed in the task execution context, without write access to DAG files. This issue affects Pig Provider versions prior to 4.0.0. It also impacts any Apache Airflow versions prior to 2.3.0 in case Pig Provider is installed (Pig Provider 4.0.0 can only be installed for Airflow 2.3.0+). Note that you need to manually install the Pig Provider version 4.0.0 in order to get rid of the vulnerability on top of Airflow 2.3.0+ version.	9.8	More Details
CVE-2022-38649	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Apache Airflow Pinot Provider, Apache Airflow allows an attacker to control commands executed in the task execution context, without write access to DAG files. This issue affects Apache Airflow Pinot Provider versions prior to 4.0.0. It also impacts any Apache Airflow versions prior to 2.3.0 in case Apache Airflow Pinot Provider is installed (Apache Airflow Pinot Provider 4.0.0 can only be installed for Airflow 2.3.0+). Note that you need to manually install the Pinot Provider version 4.0.0 in order to get rid of the vulnerability on top of Airflow 2.3.0+ version.	9.8	More Details
CVE-2022-40602	A flaw in the Zyxel LTE3301-M209 firmware verisons prior to V1.00(ABLG.6)C0 could allow a remote attacker to access the device using an improper pre-configured password if the remote administration feature has been enabled by an authenticated administrator.	9.8	More Details
CVE-2022-2166	Improper Restriction of Excessive Authentication Attempts in GitHub repository mastodon/mastodon prior to 4.0.0.	9.8	More Details
CVE-2022-44188	Netgear R7000P V1.3.0.8 is vulnerable to Buffer Overflow in /usr/sbin/httpd via parameter enable_band_steering.	9.8	More Details
CVE-2022-43214	Billing System Project v1.0 was discovered to contain a SQL injection vulnerability via the orderId parameter at printOrder.php.	9.8	More Details
CVE-2022-41326	The web conferencing component of Mitel MiCollab through 9.6.0.13 could allow an unauthenticated attacker to upload arbitrary scripts due to improper authorization controls. A successful exploit could allow remote code execution within the context of the application.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36179	Fusiondirectory 1.3 suffers from Improper Session Handling.	9.8	More Details
CVE-2022-44785	An issue was discovered in Appalti & Contratti 9.12.2. The target web applications are subject to multiple SQL Injection vulnerabilities, some of which executable even by unauthenticated users, as demonstrated by the GetListaEnti.do cfamm parameter.	9.8	More Details
CVE-2022-30258	An issue was discovered in Technitium DNS Server through 8.0.2 that allows variant V2 of unintended domain name resolution. A revoked domain name can still be resolvable for a long time, including expired domains and taken-down malicious domains. The effects of an exploit would be widespread and highly impactful, because the exploitation conforms to de facto DNS specifications and operational practices, and overcomes current mitigation patches for "Ghost" domain names.	9.8	More Details
CVE-2022-30257	An issue was discovered in Technitium DNS Server through 8.0.2 that allows variant V1 of unintended domain name resolution. A revoked domain name can still be resolvable for a long time, including expired domains and taken-down malicious domains. The effects of an exploit would be widespread and highly impactful, because the exploitation conforms to de facto DNS specifications and operational practices, and overcomes current mitigation patches for "Ghost" domain names.	9.8	More Details
CVE-2022-44183	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via function formSetWifiGuestBasic.	9.8	More Details
CVE-2022-44180	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via function addWifiMacFilter.	9.8	More Details
CVE-2022-43215	Billing System Project v1.0 was discovered to contain a SQL injection vulnerability via the endDate parameter at getOrderReport.php.	9.8	More Details
CVE-2022-44190	Netgear R7000P V1.3.1.64 is vulnerable to Buffer Overflow via parameter enable_band_steering.	9.8	More Details
CVE-2022-45047	Class org.apache.sshd.server.keyprovider.SimpleGeneratorHostKeyProvider in Apache MINA SSHD <= 2.9.1 uses Java deserialization to load a serialized java.security.PrivateKey. The class is one of several implementations that an implementor using Apache MINA SSHD can choose for loading the host keys of an SSH server.	9.8	More Details
CVE-2022-44191	Netgear R7000P V1.3.1.64 is vulnerable to Buffer Overflow via parameters KEY1 and KEY2.	9.8	More Details
CVE-2022-43212	Billing System Project v1.0 was discovered to contain a SQL injection vulnerability via the orderId parameter at fetchOrderData.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39070	There is an access control vulnerability in some ZTE PON OLT products. Due to improper access control settings, remote attackers could use the vulnerability to log in to the device and execute any operation.	9.8	More Details
CVE-2022-44808	A command injection vulnerability has been found on D-Link DIR-823G devices with firmware version 1.02B03 that allows an attacker to execute arbitrary operating system commands through well-designed /HNAP1 requests. Before the HNAP API function can process the request, the system function executes an untrusted command that triggers the vulnerability.	9.8	More Details
CVE-2022-44807	D-Link DIR-882 1.10B02 and 1.20B06 is vulnerable to Buffer Overflow via webGetVarString.	9.8	More Details
CVE-2022-44806	D-Link DIR-882 1.10B02 and 1.20B06 is vulnerable to Buffer Overflow.	9.8	More Details
CVE-2022-44804	D-Link DIR-882 1.10B02 and1.20B06 is vulnerable to Buffer Overflow via the websRedirect function.	9.8	More Details
CVE-2022-44801	D-Link DIR-878 1.02B05 is vulnerable to Incorrect Access Control.	9.8	More Details
CVE-2022-44202	D-Link DIR878 1.02B04 and 1.02B05 are vulnerable to Buffer Overflow.	9.8	More Details
CVE-2022-44201	D-Link DIR823G 1.02B05 is vulnerable to Commad Injection.	9.8	More Details
CVE-2022-44184	Netgear R7000P V1.3.0.8 is vulnerable to Buffer Overflow in /usr/sbin/httpd via parameter wan_dns1_sec.	9.8	More Details
CVE-2022-44200	Netgear R7000P V1.3.0.8, V1.3.1.64 is vulnerable to Buffer Overflow via parameters: stamode_dns1_pri and stamode_dns1_sec.	9.8	More Details
CVE-2022-44199	Netgear R7000P V1.3.1.64 is vulnerable to Buffer Overflow via parameter openvpn_server_ip.	9.8	More Details
CVE-2022-44198	Netgear R7000P V1.3.1.64 is vulnerable to Buffer Overflow via parameter openvpn_push1.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44197	Netgear R7000P V1.3.0.8 is vulnerable to Buffer Overflow via parameter openvpn_server_ip.	9.8	More Details
CVE-2022-44196	Netgear R7000P V1.3.0.8 is vulnerable to Buffer Overflow via parameter openvpn_push1.	9.8	More Details
CVE-2022-44194	Netgear R7000P V1.3.0.8 is vulnerable to Buffer Overflow via parameters apmode_dns1_pri and apmode_dns1_sec.	9.8	More Details
CVE-2022-44193	Netgear R7000P V1.3.1.64 is vulnerable to Buffer Overflow in /usr/sbin/httpd via parameters: starthour, startminute , endhour, and endminute.	9.8	More Details
CVE-2022-44178	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow. via function formWifiWpsOOB.	9.8	More Details
CVE-2022-44177	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via function formWifiWpsStart.	9.8	More Details
CVE-2022-44176	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via function fromSetRouteStatic.	9.8	More Details
CVE-2022-44004	An issue was discovered in BACKCLICK Professional 5.9.63. Due to insecure design or lack of authentication, unauthenticated attackers can complete the password-reset process for any account and set a new password.	9.8	More Details
CVE-2022-36784	Elsight – Elsight Halo Remote Code Execution (RCE) Elsight Halo web panel allows us to perform connection validation. through the POST request : /api/v1/nics/wifi/wlan0/ping we can abuse DESTINATION parameter and leverage it to remote code execution.	9.8	More Details
CVE-2022-44001	An issue was discovered in BACKCLICK Professional 5.9.63. User authentication for accessing the CORBA back-end services can be bypassed.	9.8	More Details
CVE-2022-43138	Dolibarr Open Source ERP & CRM for Business before v14.0.1 allows attackers to escalate privileges via a crafted API.	9.8	More Details
CVE-2022-42245	Dreamer CMS 4.0.01 is vulnerable to SQL Injection.	9.8	More Details
CVE-2022-40881	SolarView Compact 6.00 was discovered to contain a command injection vulnerability via network_test.php	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43782	Affected versions of Atlassian Crowd allow an attacker to authenticate as the crowd application via security misconfiguration and subsequent ability to call privileged endpoints in Crowd's REST API under the {{usermanagement}} path. This vulnerability can only be exploited by IPs specified under the crowd application allowlist in the Remote Addresses configuration, which is {{none}} by default. The affected versions are all versions 3.x.x, versions 4.x.x before version 4.4.4, and versions 5.x.x before 5.0.3	9.8	More Details
CVE-2022-43781	There is a command injection vulnerability using environment variables in Bitbucket Server and Data Center. An attacker with permission to control their username can exploit this issue to execute arbitrary code on the system. This vulnerability can be unauthenticated if the Bitbucket Server and Data Center instance has enabled “Allow public signup”.	9.8	More Details
CVE-2022-44006	An issue was discovered in BACKCLICK Professional 5.9.63. Due to improper validation or sanitization of upload filenames, an externally reachable, unauthenticated update function permits writing files outside the intended target location. Achieving remote code execution is possible, e.g., by uploading an executable file.	9.8	More Details
CVE-2022-44003	An issue was discovered in BACKCLICK Professional 5.9.63. Due to insufficient escaping of user-supplied input, the application is vulnerable to SQL injection at various locations.	9.8	More Details
CVE-2022-44175	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via function formSetMacFilterCfg.	9.8	More Details
CVE-2022-44000	An issue was discovered in BACKCLICK Professional 5.9.63. Due to an exposed internal communications interface, it is possible to execute arbitrary system commands on the server.	9.8	More Details
CVE-2022-40752	IBM InfoSphere DataStage 11.7 is vulnerable to a command injection vulnerability due to improper neutralization of special elements. IBM X-Force ID: 236687.	9.8	More Details
CVE-2022-43999	An issue was discovered in BACKCLICK Professional 5.9.63. Due to exposed CORBA management services, arbitrary system commands can be executed on the server.	9.8	More Details
CVE-2022-43135	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the username parameter at /diagnostic/login.php.	9.8	More Details
CVE-2022-43262	Human Resource Management System v1.0 was discovered to contain a SQL injection vulnerability via the password parameter at /hrm/controller/login.php.	9.8	More Details
CVE-2022-43256	SeaCms before v12.6 was discovered to contain a SQL injection vulnerability via the component /js/player/dmplayer/dmku/index.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43234	An arbitrary file upload vulnerability in the /attachments component of Hoosk v1.8 allows attackers to execute arbitrary code via a crafted PHP file.	9.8	More Details
CVE-2022-3980	An XML External Entity (XEE) vulnerability allows server-side request forgery (SSRF) and potential code execution in Sophos Mobile managed on-premises between versions 5.0.0 and 9.7.4.	9.8	More Details
CVE-2022-36787	webvendome - webvendome SQL Injection. SQL Injection in the Parameter " DocNumber" Request : Get Request : /webvendome/showfiles.aspx?jobnumber=nullDoc Number=HERE.	9.8	More Details
CVE-2022-38165	Arbitrary file write in F-Secure Policy Manager through 2022-08-10 allows unauthenticated users to write the file with the contents in arbitrary locations on the F-Secure Policy Manager Server.	9.8	More Details
CVE-2022-39180	College Management System v1.0 - SQL Injection (SQLi). By inserting SQL commands to the username and password fields in the login.php page	9.8	More Details
CVE-2022-4093	SQL injection attacks can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information. Many high-profile data breaches in recent years have been the result of SQL injection attacks, leading to reputational damage and regulatory fines. In some cases, an attacker can obtain a persistent backdoor into an organization's systems, leading to a long-term compromise that can go unnoticed for an extended period. This affect 16.0.1 and 16.0.2 only. 16.0.0 or lower, and 16.0.3 or higher are not affected	9.8	More Details
CVE-2022-44174	Tenda AC18 V15.03.05.05 is vulnerable to Buffer Overflow via function formSetDeviceName.	9.8	More Details
CVE-2022-44172	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via function R7WebsSecurityHandler.	9.8	More Details
CVE-2022-44171	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via function form_fast_setting_wifi_set.	9.8	More Details
CVE-2022-3634	The Contact Form 7 Database Addon WordPress plugin before 1.2.6.5 does not validate data when output it back in a CSV file, which could lead to CSV injection	9.8	More Details
CVE-2022-3600	The Easy Digital Downloads WordPress plugin before 3.1.0.2 does not validate data when its output in a CSV file, which could lead to CSV injection.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24649	The WP User Frontend WordPress plugin before 3.5.29 uses a user supplied argument called urhidden in its registration form, which contains the role for the account to be created with, encrypted via wpuf_encryption(). This could allow an attacker having access to the AUTH_KEY and AUTH_SALT constant (via an arbitrary file access issue for example, or if the blog is using the default keys) to create an account with any role they want, such as admin	9.8	More Details
CVE-2022-44204	D-Link DIR3060 DIR3060A1_FW111B04.bin is vulnerable to Buffer Overflow.	9.8	More Details
CVE-2022-4116	A vulnerability was found in quarkus. This security flaw happens in Dev UI Config Editor which is vulnerable to drive-by localhost attacks leading to remote code execution.	9.8	More Details
CVE-2022-4070	Insufficient Session Expiration in GitHub repository librenms/librenms prior to 22.10.0.	9.8	More Details
CVE-2022-45132	In Linaro Automated Validation Architecture (LAVA) before 2022.11.1, remote code execution can be achieved through user-submitted Jinja2 template. The REST API endpoint for validating device configuration files in lava-server loads input as a Jinja2 template in a way that can be used to trigger remote code execution in the LAVA server.	9.8	More Details
CVE-2022-42698	Unauth. Arbitrary File Upload vulnerability in WordPress Api2Cart Bridge Connector plugin <= 1.1.0 on WordPress.	9.8	More Details
CVE-2022-45474	drachtio-server 0.8.18 has a request-handler.cpp event_cb use-after-free for any request.	9.8	More Details
CVE-2022-41937	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. The application allows anyone with view access to modify any page of the wiki by importing a crafted XAR package. The problem has been patched in XWiki 14.6RC1, 14.6 and 13.10.8. As a workaround, setting the right of the page Filter.WebHome and making sure only the main wiki administrators can view the application installed on main wiki or edit the page and apply the changed described in commit fb49b4f.	9.6	More Details
CVE-2022-36180	Fusiondirectory 1.3 is vulnerable to Cross Site Scripting (XSS) via /fusiondirectory/index.php?message=[injection], /fusiondirectory/index.php?message=invalidparameter&plug={Injection], /fusiondirectory/index.php?signout=1&message=[injection]&plug=106.	9.6	More Details
CVE-2022-43143	A cross-site scripting (XSS) vulnerability in Beekeeper Studio v3.6.6 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the error modal container.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44584	Unauth. Arbitrary File Deletion vulnerability in WatchTowerHQ plugin <= 3.6.15 on WordPress.	9.1	More Details
CVE-2022-40842	ndk design NdkAdvancedCustomizationFields 3.5.0 is vulnerable to Server-side request forgery (SSRF) via rotateimg.php.	9.1	More Details
CVE-2022-41938	Flarum is an open source discussion platform. Flarum's page title system allowed for page titles to be converted into HTML DOM nodes when pages were rendered. The change was made after `v1.5` and was not noticed. This allowed an attacker to inject malicious HTML markup using a discussion title input, either by creating a new discussion or renaming one. The XSS attack occurs after a visitor opens the relevant discussion page. All communities running Flarum from `v1.5.0` to `v1.6.1` are impacted. The vulnerability has been fixed and published as flarum/core `v1.6.2`. All communities running Flarum from `v1.5.0` to `v1.6.1` have to upgrade as soon as possible to v1.6.2. There are no known workarounds for this issue.	9.0	More Details
CVE-2022-42989	ERP Sankhya before v4.11b81 was discovered to contain a cross-site scripting (XSS) vulnerability via the component Caixa de Entrada.	9.0	More Details
CVE-2022-41943	sourcegraph is a code intelligence platform. As a site admin it was possible to execute arbitrary commands on Gitserver when the experimental `customGitFetch` feature was enabled. This experimental feature has now been disabled by default. This issue has been patched in version 4.1.0.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-44784	An issue was discovered in Appalti & Contratti 9.12.2. The target web applications LFS and DL229 expose a set of services provided by the Axis 1.4 instance, embedded directly into the applications, as hinted by the WEB-INF/web.xml file leaked through Local File Inclusion. Among the exposed services, there is the Axis AdminService, which, through the default configuration, should normally be accessible only by the localhost. Nevertheless, by trying to access the mentioned service, both in LFS and DL229, the service can actually be reached even by remote users, allowing creation of arbitrary services on the server side. When an attacker can reach the AdminService, they can use it to instantiate arbitrary services on the server. The exploit procedure is well known and described in Generic AXIS-SSRF exploitation. Basically, the attack consists of writing a JSP page inside the root directory of the web application, through the org.apache.axis.handlers.LogHandler class.	8.8	More Details
CVE-2022-39066	There is a SQL injection vulnerability in ZTE MF286R. Due to insufficient validation of the input parameters of the phonebook interface, an authenticated attacker could use the vulnerability to execute arbitrary SQL injection.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42098	KLiK SocialMediaWebsite version v1.0.1 is vulnerable to SQL Injection via the profile.php.	8.8	More Details
CVE-2022-44007	An issue was discovered in BACKCLICK Professional 5.9.63. Due to an unsafe implementation of session tracking, it is possible for an attacker to trick users into opening an authenticated user session for a session identifier known to the attacker, aka Session Fixation.	8.8	More Details
CVE-2021-38819	A SQL injection vulnerability exits on the Simple Image Gallery System 1.0 application through "id" parameter on the album page.	8.8	More Details
CVE-2022-42246	Doufox 0.0.4 contains a CSRF vulnerability that can add system administrator account.	8.8	More Details
CVE-2022-3688	The WPQA Builder WordPress plugin before 5.9 does not have CSRF check when following and unfollowing users, which could allow attackers to make logged in users perform such actions via CSRF attacks	8.8	More Details
CVE-2022-44384	An arbitrary file upload vulnerability in rconfig v3.9.6 allows attackers to execute arbitrary code via a crafted PHP file.	8.8	More Details
CVE-2022-38148	Silverstripe silverstripe/framework through 4.11 allows SQL Injection.	8.8	More Details
CVE-2022-43506	SQL Injection in HandlerTag_KID.ashx in Delta Electronics DIAEnergie versions prior to v1.9.02.001 allows an attacker to inject SQL queries via Network	8.8	More Details
CVE-2022-3861	The Betheme theme for WordPress is vulnerable to PHP Object Injection in versions up to, and including, 26.5.1.4 via deserialization of untrusted input supplied via the import, mfn-items-import-page, and mfn-items-import parameters passed through the mfn_builder_import, mfn_builder_import_page, importdata, importsinglepage, and importfromclipboard functions. This makes it possible for authenticated attackers, with contributor level permissions and above to inject a PHP Object. The additional presence of a POP chain would make it possible for attackers to execute code, retrieve sensitive data, delete files, etc..	8.8	More Details
CVE-2022-43457	SQL Injection in HandlerPage_KID.ashx in Delta Electronics DIAEnergie versions prior to v1.9.02.001 allows an attacker to inject SQL queries via Network	8.8	More Details
CVE-2022-43452	SQL Injection in FtyInfoSetting.aspx in Delta Electronics DIAEnergie versions prior to v1.9.02.001 allows an attacker to inject SQL queries via Network	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43447	SQL Injection in AM_EBillAnalysis.aspx in Delta Electronics DIAEnergie versions prior to v1.9.02.001 allows an attacker to inject SQL queries via Network	8.8	More Details
CVE-2022-43183	XXL-Job before v2.3.1 contains a Server-Side Request Forgery (SSRF) via the component /admin/controller/JobLogController.java.	8.8	More Details
CVE-2021-33621	The cgi gem before 0.1.0.2, 0.2.x before 0.2.2, and 0.3.x before 0.3.5 for Ruby allows HTTP response splitting. This is relevant to applications that use untrusted user input either to generate an HTTP response or to create a CGI::Cookie object.	8.8	More Details
CVE-2022-41775	SQL Injection in Handler_CFG.ashx in Delta Electronics DIAEnergie versions prior to v1.9.02.001 allows an attacker to inject SQL queries via Network	8.8	More Details
CVE-2022-43685	CKAN through 2.9.6 account takeovers by unauthenticated users when an existing user id is sent via an HTTP POST request. This allows a user to take over an existing account including superuser accounts.	8.8	More Details
CVE-2022-36924	The Zoom Rooms Installer for Windows prior to 5.12.6 contains a local privilege escalation vulnerability. A local low-privileged user could exploit this vulnerability during the install process to escalate their privileges to the SYSTEM user.	8.8	More Details
CVE-2022-33012	Microweber v1.2.15 was discovered to allow attackers to perform an account takeover via a host header injection attack.	8.8	More Details
CVE-2022-28768	The Zoom Client for Meetings Installer for macOS (Standard and for IT Admin) before version 5.12.6 contains a local privilege escalation vulnerability. A local low-privileged user could exploit this vulnerability during the install process to escalate their privileges to root.	8.8	More Details
CVE-2022-1578	The My wpdb WordPress plugin before 2.5 is missing CSRF check when running SQL queries, which could allow attacker to make a logged in admin run arbitrary SQL query via a CSRF attack	8.8	More Details
CVE-2022-3525	Deserialization of Untrusted Data in GitHub repository librenms/librenms prior to 22.10.0.	8.8	More Details
CVE-2022-3388	An input validation vulnerability exists in the Monitor Pro interface of MicroSCADA Pro and MicroSCADA X SYS600. An authenticated user can launch an administrator level remote code execution irrespective of the authenticated user's role.	8.8	More Details
CVE-2022-4021	The Permalink Manager Lite plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.2.20.1. This is due to missing or incorrect nonce validation on the extra_actions function. This makes it possible for unauthenticated attackers to change plugin settings including permalinks and site maps, via forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24036	Karmasis Informatics Infraskope SIEM+ has an unauthenticated access vulnerability which could allow an unauthenticated attacker to modificate logs.	8.6	More Details
CVE-2022-24037	Karmasis Informatics Infraskope SIEM+ has an unauthenticated access vulnerability which could allow an unauthenticated attacker to obtain critical information.	8.2	More Details
CVE-2022-39389	Lightning Network Daemon (lnd) is an implementation of a lightning bitcoin overlay network node. All lnd nodes before version `v0.15.4` are vulnerable to a block parsing bug that can cause a node to enter a degraded state once encountered. In this degraded state, nodes can continue to make payments and forward HTLCs, and close out channels. Opening channels is prohibited, and also on chain transaction events will be undetected. This can cause loss of funds if a CSV expiry is researched during a breach attempt or a CLTV delta expires forgetting the funds in the HTLC. A patch is available in `lnd` version 0.15.4. Users are advised to upgrade. Users unable to upgrade may use the `lncli updatechanpolicy` RPC call to increase their CLTV value to a very high amount or increase their fee policies. This will prevent nodes from routing through your node, meaning that no pending HTLCs can be present.	8.2	More Details
CVE-2022-3589	An API Endpoint used by Miele's "AppWash" MobileApp in all versions was vulnerable to an authorization bypass. A low privileged, remote attacker would have been able to gain read and partial write access to other users data by modifying a small part of a HTTP request sent to the API. Reading or changing the password of another user was not possible, thus no impact to Availability.	8.1	More Details
CVE-2022-3763	The Booster for WooCommerce WordPress plugin before 5.6.7, Booster Plus for WooCommerce WordPress plugin before 5.6.5, Booster Elite for WooCommerce WordPress plugin before 1.1.7 do not have CSRF check in place when deleting files uploaded at the checkout, allowing attackers to make a logged in shop manager or admin delete them via a CSRF attack	8.1	More Details
CVE-2022-41942	Sourcegraph is a code intelligence platform. In versions prior to 4.1.0 a command Injection vulnerability existed in the gitserver service, present in all Sourcegraph deployments. This vulnerability was caused by a lack of input validation on the host parameter of the `/list-gitolite` endpoint. It was possible to send a crafted request to gitserver that would execute commands inside the container. Successful exploitation requires the ability to send local requests to gitserver. The issue is patched in version 4.1.0.	7.9	More Details
CVE-2022-3910	Use After Free vulnerability in Linux Kernel allows Privilege Escalation. An improper Update of Reference Count in io_uring leads to Use-After-Free and Local Privilege Escalation. When io_msg_ring was invoked with a fixed file, it called io_fput_file() which improperly decreased its reference count (leading to Use-After-Free and Local Privilege Escalation). Fixed files are permanently registered to the ring, and should not be put separately. We recommend upgrading past commit https://github.com/torvalds/linux/commit/fc7222c3a9f56271fba02aabbfbae999042f1679 https://github.com/torvalds/linux/commit/fc7222c3a9f56271fba02aabbfbae999042f1679	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44830	Sourcecodester Event Registration App v1.0 was discovered to contain multiple CSV injection vulnerabilities via the First Name, Contact and Remarks fields. These vulnerabilities allow attackers to execute arbitrary code via a crafted excel file.	7.8	More Details
CVE-2022-31608	NVIDIA GPU Display Driver for Linux contains a vulnerability in an optional D-Bus configuration file, where a local user with basic capabilities can impact protected D-Bus endpoints, which may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2022-38097	A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 12.0.1.12430. By prematurely destroying annotation objects, a specially-crafted PDF document can trigger the reuse of previously freed memory, which can lead to arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially-crafted, malicious site if the browser plugin extension is enabled.	7.8	More Details
CVE-2022-31610	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds write, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.	7.8	More Details
CVE-2022-41131	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Apache Airflow Hive Provider, Apache Airflow allows an attacker to execute arbtrary commands in the task execution context, without write access to DAG files. This issue affects Hive Provider versions prior to 4.1.0. It also impacts any Apache Airflow versions prior to 2.3.0 in case HIve Provider is installed (Hive Provider 4.1.0 can only be installed for Airflow 2.3.0+). Note that you need to manually install the HIve Provider version 4.1.0 in order to get rid of the vulnerability on top of Airflow 2.3.0+ version that has lower version of the Hive Provider installed).	7.8	More Details
CVE-2022-40129	A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 12.0.1.12430. A specially-crafted PDF document can trigger the reuse of previously freed memory via misusing Optional Content Group API, which can lead to arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially-crafted, malicious site if the browser plugin extension is enabled.	7.8	More Details
CVE-2022-45422	When LG SmartShare is installed, local privilege escalation is possible through DLL Hijacking attack. The LG ID is LVE-HOT-220005.	7.8	More Details
CVE-2022-43308	INTELBRAS SG 2404 MR 20180928-rel64938 allows authenticated attackers to arbitrarily create Administrator accounts via crafted user cookies.	7.8	More Details
CVE-2022-42533	In shared_metadata_init of SharedMetadata.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239415718References: N/A	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44725	OPC Foundation Local Discovery Server (LDS) through 1.04.403.478 uses a hard-coded file path to a configuration file. This allows a normal user to create a malicious file that is loaded by LDS (running as a high-privilege user).	7.8	More Details
CVE-2022-32774	A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 12.0.1.12430. By prematurely deleting objects associated with pages, a specially-crafted PDF document can trigger the reuse of previously freed memory, which can lead to arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially-crafted, malicious site if the browser plugin extension is enabled.	7.8	More Details
CVE-2022-35407	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. A stack buffer overflow leads to arbitrary code execution in the SetupUtility driver on Intel platforms. An attacker can change the values of certain UEFI variables. If the size of the second variable exceeds the size of the first, then the buffer will be overwritten. This issue affects the SetupUtility driver of InsydeH2O.	7.8	More Details
CVE-2022-37332	A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 12.0.1.12430. A specially-crafted PDF document can trigger the reuse of previously freed memory via misusing media player API, which can lead to arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially-crafted, malicious site if the browser plugin extension is enabled.	7.8	More Details
CVE-2022-31606	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a failure to properly validate data might allow an attacker with basic user capabilities to cause an out-of-bounds access in kernel mode, which could lead to denial of service, information disclosure, escalation of privileges, or data tampering.	7.8	More Details
CVE-2022-31617	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds read, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.	7.8	More Details
CVE-2022-31607	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer (nvidia.ko), where a local user with basic capabilities can cause improper input validation, which may lead to denial of service, escalation of privileges, data tampering, and limited information disclosure.	7.8	More Details
CVE-2022-23748	mDNSResponder.exe is vulnerable to DLL Sideloading attack. Executable improperly specifies how to load the DLL, from which folder and under what conditions. In these scenarios, a malicious attacker could be using the valid and legitimate executable to load malicious files.	7.8	More Details
CVE-2022-37197	IOBit IOTransfer V4 is vulnerable to Unquoted Service Path.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36785	D-Link – G integrated Access Device4 Information Disclosure & Authorization Bypass. *Information Disclosure – file contains a URL with private IP at line 15 "login.asp" A. The window.location.href = http://192.168.1.1/setupWizard.asp" http://192.168.1.1/setupWizard.asp" ; "admin" – contains default username value "login.asp" B. While accessing the web interface, the login form at *Authorization Bypass – URL by "setupWizard.asp' while it blocks direct access to – the web interface does not properly validate user identity variables values located at the client side, it is available to access it without a "login_glag" and "login_status" checking browser and to read the admin user credentials for the web interface.	7.5	More Details
CVE-2022-45331	AeroCMS v0.0.1 was discovered to contain a SQL Injection vulnerability via the p_id parameter at \post.php. This vulnerability allows attackers to access database information.	7.5	More Details
CVE-2022-38871	In Free5gc v3.0.5, the AMF breaks due to malformed NAS messages.	7.5	More Details
CVE-2022-44169	Tenda AC15 V15.03.05.18 is vulnerable to Buffer Overflow via function formSetVirtualSer.	7.5	More Details
CVE-2022-44168	Tenda AC15 V15.03.05.18 is vulnerable to Buffer Overflow via function fromSetRouteStatic..	7.5	More Details
CVE-2022-3090	Red Lion Controls Crimson 3.0 versions 707.000 and prior, Crimson 3.1 versions 3126.001 and prior, and Crimson 3.2 versions 3.2.0044.0 and prior are vulnerable to path traversal. When attempting to open a file using a specific path, the user's password hash is sent to an arbitrary host. This could allow an attacker to obtain user credential hashes.	7.5	More Details
CVE-2022-45330	AeroCMS v0.0.1 was discovered to contain a SQL Injection vulnerability via the Category parameter at \category.php. This vulnerability allows attackers to access database information.	7.5	More Details
CVE-2022-44786	An issue was discovered in Appalti & Contratti 9.12.2. The target web applications allow Local File Inclusion in any page relying on the href parameter to specify the JSP page to be rendered. This affects ApriPagina.do POST and GET requests to each application.	7.5	More Details
CVE-2022-44167	Tenda AC15 V15.03.05.18 is avulnerable to Buffer Overflow via function formSetPPTPServer.	7.5	More Details
CVE-2022-44163	Tenda AC21 V16.03.08.15 is vulnerable to Buffer Overflow via function formSetMacFilterCfg.	7.5	More Details
CVE-2022-43264	Arobas Music Guitar Pro for iPad and iPhone before v1.10.2 allows attackers to perform directory traversal and download arbitrary files via a crafted web request.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42732	A vulnerability has been identified in syngo Dynamics (All versions < VA40G HF01). syngo Dynamics application server hosts a web service using an operation with improper read access control that could allow files to be retrieved from any folder accessible to the account assigned to the website’s application pool.	7.5	More Details
CVE-2022-30256	An issue was discovered in MaraDNS Deadwood through 3.5.0021 that allows variant V1 of unintended domain name resolution. A revoked domain name can still be resolvable for a long time, including expired domains and taken-down malicious domains. The effects of an exploit would be widespread and highly impactful, because the exploitation conforms to de facto DNS specifications and operational practices, and overcomes current mitigation patches for "Ghost" domain names.	7.5	More Details
CVE-2022-1579	The function check_is_login_page() uses headers for the IP check, which can be easily spoofed.	7.5	More Details
CVE-2022-41840	Unauth. Directory Traversal vulnerability in Welcart eCommerce plugin <= 2.7.7 on WordPress.	7.5	More Details
CVE-2022-3691	The DeepL Pro API translation plugin WordPress plugin before 1.7.5 discloses sensitive information (including the DeepL API key) in files that are publicly accessible to an external, unauthenticated visitor.	7.5	More Details
CVE-2022-42982	BKG Professional NtripCaster 2.0.39 allows querying information over the UDP protocol without authentication. The NTRIP sourcetable is typically quite long (tens of kBs) and can be requested with a packet of only 30 bytes. This presents a vector that can be used for UDP amplification attacks. Normally, only authenticated streaming data will be provided over UDP and not the sourcetable.	7.5	More Details
CVE-2022-44583	Unauth. Arbitrary File Download vulnerability in WatchTowerHQ plugin <= 3.6.15 on WordPress.	7.5	More Details
CVE-2022-44158	Tenda AC21 V16.03.08.15 is vulnerable to Buffer Overflow via function via set_device_name.	7.5	More Details
CVE-2022-0222	A CWE-269: Improper Privilege Management vulnerability exists that could cause a denial of service of the Ethernet communication of the controller when sending a specific request over SNMP. Affected products: Modicon M340 CPUs(BMXP34* versions prior to V3.40), Modicon M340 X80 Ethernet Communication modules:BMXNOE0100 (H), BMXNOE0110 (H), BMXNOR0200H RTU(BMXNOE* all versions)(BMXNOR* versions prior to v1.7 IR24)	7.5	More Details
CVE-2022-42733	A vulnerability has been identified in syngo Dynamics (All versions < VA40G HF01). syngo Dynamics application server hosts a web service using an operation with improper read access control that could allow files to be retrieved from any folder accessible to the account assigned to the website’s application pool.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42734	A vulnerability has been identified in syngo Dynamics (All versions < VA40G HF01). syngo Dynamics application server hosts a web service using an operation with improper write access control that could allow to write data in any folder accessible to the account assigned to the website's application pool.	7.5	More Details
CVE-2022-42891	A vulnerability has been identified in syngo Dynamics (All versions < VA40G HF01). syngo Dynamics application server hosts a web service using an operation with improper write access control that could allow to write data in any folder accessible to the account assigned to the website's application pool.	7.5	More Details
CVE-2022-37301	A CWE-191: Integer Underflow (Wrap or Wraparound) vulnerability exists that could cause a denial of service of the controller due to memory access violations when using the Modbus TCP protocol. Affected products: Modicon M340 CPU (part numbers BMXP34*)(V3.40 and prior), Modicon M580 CPU (part numbers BMEP* and BMEH*)(V3.22 and prior), Legacy Modicon Quantum/Premium(All Versions), Modicon Momentum MDI (171CBU*)(All Versions), Modicon MC80 (BMKC80)(V1.7 and prior)	7.5	More Details
CVE-2022-42893	A vulnerability has been identified in syngo Dynamics (All versions < VA40G HF01). syngo Dynamics application server hosts a web service using an operation with improper write access control that could allow to write data in any folder accessible to the account assigned to the website's application pool.	7.5	More Details
CVE-2022-42894	A vulnerability has been identified in syngo Dynamics (All versions < VA40G HF01). An unauthenticated Server-Side Request Forgery (SSRF) vulnerability was identified in one of the web services exposed on the syngo Dynamics application that could allow for the leaking of NTLM credentials as well as local service enumeration.	7.5	More Details
CVE-2022-43140	kkFileView v4.1.0 was discovered to contain a Server-Side Request Forgery (SSRF) via the component cn.keking.web.controller.OnlinePreviewController#getCorsFile. This vulnerability allows attackers to force the application to make arbitrary requests via injection of crafted URLs into the url parameter.	7.5	More Details
CVE-2022-45470	missing input validation in Apache Hama may cause information disclosure through path traversal and XSS. Since Apache Hama is EOL, we do not expect these issues to be fixed.	7.5	More Details
CVE-2022-44156	Tenda AC15 V15.03.05.19 is vulnerable to Buffer Overflow via function formSetIpMacBind.	7.5	More Details
CVE-2022-45461	The Java Admin Console in Veritas NetBackup through 10.1 and related Veritas products on Linux and UNIX allows authenticated non-root users (that have been explicitly added to the auth.conf file) to execute arbitrary commands as root.	7.5	More Details
CVE-2022-4055	When xdg-mail is configured to use thunderbird for mailto URLs, improper parsing of the URL can lead to additional headers being passed to thunderbird that should not be included per RFC 2368. An attacker can use this method to create a mailto URL that looks safe to users, but will actually attach files when clicked.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31694	InstallBuilder Qt installers built with versions previous to 22.10 try to load DLLs from the installer binary parent directory when displaying popups. This may allow an attacker to plant a malicious DLL in the installer parent directory to allow executing code with the privileges of the installer (when the popup triggers the loading of the library). Exploiting these type of vulnerabilities generally require that an attacker has access to a vulnerable machine to plant the malicious DLL.	7.3	More Details
CVE-2022-37931	A vulnerability in NetBatch-Plus software allows unauthorized access to the application. HPE has provided a workaround and fix. Please refer to HPE Security Bulletin HPESBNS04388 for details.	7.3	More Details
CVE-2022-43179	Online Leave Management System v1.0 was discovered to contain a SQL injection vulnerability via the component /admin/?page=user/manage_user&id=.	7.2	More Details
CVE-2022-44413	Automotive Shop Management System v1.0 is vulnerable to SQL Injection via /asms/admin/mechanics/manage_mechanic.php?id=.	7.2	More Details
CVE-2022-44415	Automotive Shop Management System v1.0 is vulnerable to SQL Injection via /asms/admin/mechanics/view_mechanic.php?id=.	7.2	More Details
CVE-2022-44379	Automotive Shop Management System v1.0 is vulnerable to SQL Injection via /asms/classes/Master.php?f=delete_service.	7.2	More Details
CVE-2022-44820	Automotive Shop Management System v1.0 is vulnerable to SQL Injection via /asms/admin/?page=transactions/manage_transaction&id=.	7.2	More Details
CVE-2022-3720	The Event Monster WordPress plugin before 1.2.0 does not validate and escape some parameters before using them in SQL statements, which could lead to SQL Injection exploitable by high privilege users	7.2	More Details
CVE-2022-44414	Automotive Shop Management System v1.0 is vulnerable to SQL Injection via /asms/admin/services/manage_service.php?id=.	7.2	More Details
CVE-2022-42459	Auth. WordPress Options Change vulnerability in Image Hover Effects Ultimate plugin <= 9.7.1 on WordPress.	7.2	More Details
CVE-2022-44402	Automotive Shop Management System v1.0 is vulnerable to SQL Injection via /asms/classes/Master.php?f=delete_transaction.	7.2	More Details
CVE-2022-44403	Automotive Shop Management System v1.0 is vulnerable to SQL Injection via /asms/admin/?page=user/manage_user&id=.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43162	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /tests/view_test.php.	7.2	More Details
CVE-2022-43163	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /clients/view_client.php.	7.2	More Details
CVE-2022-44378	Automotive Shop Management System v1.0 is vulnerable to SQL via /asms/classes/Master.php?f=delete_mechanic.	7.2	More Details
CVE-2022-30529	File upload vulnerability in asith-eranga ISIC tour booking through version published on Feb 13th 2018, allows attackers to upload arbitrary files via /system/application/libs/js/tinymce/plugins/filemanager/dialog.php and /system/application/libs/js/tinymce/plugins/filemanager/upload.php.	7.2	More Details
CVE-2022-42904	Zoho ManageEngine ADManager Plus through 7151 allows authenticated admin users to execute the commands in proxy settings.	7.2	More Details
CVE-2022-39179	College Management System v1.0 - Authenticated remote code execution. An admin user (the authentication can be bypassed using SQL Injection that mentioned in my other report) can upload .php file that contains malicious code via student.php file.	7.2	More Details
CVE-2022-40746	IBM i Access Family 1.1.2 through 1.1.4 and 1.1.4.3 through 1.1.9.0 could allow a local authenticated attacker to execute arbitrary code on the system, caused by DLL search order hijacking vulnerability. By placing a specially crafted file in a compromised folder, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 236581.	7.2	More Details
CVE-2022-41940	Engine.IO is the implementation of transport-based cross-browser/cross-device bi-directional communication layer for Socket.IO. A specially crafted HTTP request can trigger an uncaught exception on the Engine.IO server, thus killing the Node.js process. This impacts all the users of the engine.io package, including those who uses depending packages like socket.io. There is no known workaround except upgrading to a safe version. There are patches for this issue released in versions 3.6.1 and 6.2.1.	7.1	More Details
CVE-2022-31613	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer, where any local user can cause a null-pointer dereference, which may lead to a kernel panic.	7.1	More Details
CVE-2022-2513	A vulnerability exists in the Intelligent Electronic Device (IED) Connectivity Package (ConnPack) credential storage function in Hitachi Energy's PCM600 product included in the versions listed below, where IEDs credentials are stored in a cleartext format in the PCM600 database and logs files. An attacker having get access to the exported backup file can exploit the vulnerability and obtain user credentials of the IEDs. Additionally, an attacker with administrator access to the PCM600 host machine can obtain other user credentials by analyzing database log files. The credentials may be used to perform unauthorized modifications such as loading incorrect configurations, reboot the IEDs or cause a denial-of-service on the IEDs.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41894	TensorFlow is an open source platform for machine learning. The reference kernel of the `CONV_3D_TRANSPOSE` TensorFlow Lite operator wrongly increments the data_ptr when adding the bias to the result. Instead of `data_ptr += num_channels;` it should be `data_ptr += output_num_channels;` as if the number of input channels is different than the number of output channels, the wrong result will be returned and a buffer overflow will occur if num_channels > output_num_channels. An attacker can craft a model with a specific number of input channels. It is then possible to write specific values through the bias of the layer outside the bounds of the buffer. This attack only works if the reference kernel resolver is used in the interpreter. We have patched the issue in GitHub commit 72c0bdcb25305b0b36842d746cc61d72658d2941. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.	7.1	More Details
CVE-2022-41900	TensorFlow is an open source platform for machine learning. The security vulnerability results in FractionalMax(AVG)Pool with illegal pooling_ratio. Attackers using Tensorflow can exploit the vulnerability. They can access heap memory which is not in the control of user, leading to a crash or remote code execution. We have patched the issue in GitHub commit 216525144ee7c910296f5b05d214ca1327c9ce48. The fix will be included in TensorFlow 2.11.0. We will also cherry pick this commit on TensorFlow 2.10.1.	7.1	More Details
CVE-2022-40192	Cross-Site Request Forgery (CSRF) vulnerability in wpForo Forum plugin <= 2.0.9 on WordPress.	7.1	More Details
CVE-2022-31612	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to a system crash or a leak of internal kernel information.	7.1	More Details
CVE-2022-41883	TensorFlow is an open source platform for machine learning. When ops that have specified input sizes receive a differing number of inputs, the executor will crash. We have patched the issue in GitHub commit f5381e0e10b5a61344109c1b7c174c68110f7629. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.	6.8	More Details
CVE-2022-43096	Mediatrix 4102 before v48.5.2718 allows local attackers to gain root access via the UART port.	6.8	More Details
CVE-2022-35897	An stack buffer overflow vulnerability leads to arbitrary code execution issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. If the attacker modifies specific UEFI variables, it can cause a stack overflow, leading to arbitrary code execution. The specific variables are normally locked (read-only) at the OS level and therefore an attack would require direct SPI modification. If an attacker can change the values of at least two variables out of three (SecureBootEnforce, SecureBoot, RestoreBootSettings), it is possible to execute arbitrary code.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40765	A vulnerability in the Edge Gateway component of Mitel MiVoice Connect through 19.3 (22.22.6100.0) could allow an authenticated attacker with internal network access to conduct a command-injection attack, due to insufficient restriction of URL parameters.	6.8	More Details
CVE-2022-41880	TensorFlow is an open source platform for machine learning. When the `BaseCandidateSamplerOp` function receives a value in `true_classes` larger than `range_max`, a heap oob read occurs. We have patched the issue in GitHub commit b389f5c944cadfdfe599b3f1e4026e036f30d2d4. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.	6.8	More Details
CVE-2022-41223	The Director database component of MiVoice Connect through 19.3 (22.22.6100.0) could allow an authenticated attacker to conduct a code-injection attack via crafted data due to insufficient restrictions on the database data type.	6.8	More Details
CVE-2022-43192	An arbitrary file upload vulnerability in the component /dede/file_manage_control.php of Dedecms v5.7.101 allows attackers to execute arbitrary code via a crafted PHP file. This vulnerability is related to an incomplete fix for CVE-2022-40886.	6.7	More Details
CVE-2022-20460	In (TBD) mprot_unmap? of (TBD), there is a possible way to corrupt the memory mapping due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239557547References: N/A	6.7	More Details
CVE-2022-20427	In (TBD) of (TBD), there is a possible way to corrupt memory due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239555070References: N/A	6.7	More Details
CVE-2022-20428	In (TBD) of (TBD), there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239555411References: N/A	6.7	More Details
CVE-2022-20459	In (TBD) of (TBD), there is a possible way to redirect code execution due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239556260References: N/A	6.7	More Details
CVE-2020-23582	A vulnerability in the "/admin/wlmultipleap.asp" of optilink OP-XT71000N version: V2.2 could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack to create Multiple WLAN BSSID.	6.5	More Details
CVE-2022-4011	A vulnerability was found in Simple History Plugin. It has been rated as critical. This issue affects some unknown processing of the component Header Handler. The manipulation of the argument X-Forwarded-For leads to improper output neutralization for logs. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-213785 was assigned to this vulnerability.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44641	In Linaro Automated Validation Architecture (LAVA) before 2022.11, users with valid credentials can submit crafted XMLRPC requests that cause a recursive XML entity expansion, leading to excessive use of memory on the server and a Denial of Service.	6.5	More Details
CVE-2022-44788	An issue was discovered in Appalti & Contratti 9.12.2. It allows Session Fixation. When a user logs in providing a JSESSIONID cookie that is issued by the server at the first visit, the cookie value is not updated after a successful login.	6.5	More Details
CVE-2022-34665	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service.	6.5	More Details
CVE-2022-4111	Unrestricted file size limit can lead to DoS in tooljet/tooljet <1.27 by allowing a logged in attacker to upload profile pictures over 2MB.	6.5	More Details
CVE-2022-41781	Broken Access Control vulnerability in Permalink Manager Lite plugin <= 2.2.20 on WordPress.	6.5	More Details
CVE-2022-41652	Bypass vulnerability in Quiz And Survey Master plugin <= 7.3.10 on WordPress.	6.5	More Details
CVE-2022-39067	There is a buffer overflow vulnerability in ZTE MF286R. Due to lack of input validation on parameters of the wifi interface, an authenticated attacker could use the vulnerability to perform a denial of service attack.	6.5	More Details
CVE-2022-24038	Karmasis Informatics Infraskope SIEM+ has an unauthenticated access vulnerability which could allow an unauthenticated attacker to damage the page where the agents are listed.	6.5	More Details
CVE-2022-44008	An issue was discovered in BACKCLICK Professional 5.9.63. Due to improper validation, arbitrary local files can be retrieved by accessing the back-end Tomcat server directly.	6.5	More Details
CVE-2022-3762	The Booster for WooCommerce WordPress plugin before 5.6.7, Booster Plus for WooCommerce WordPress plugin before 5.6.5, Booster Elite for WooCommerce WordPress plugin before 1.1.7 do not validate files to download in some of its modules, which could allow ShopManager and Admin to download arbitrary files from the server even when they are not supposed to be able to (for example in multisite)	6.5	More Details
CVE-2022-41135	Unauth. Plugin Settings Change vulnerability in Modula plugin <= 2.6.9 on WordPress.	6.5	More Details
CVE-2022-43171	A heap buffer overflow in the LIEF::MachO::BinaryParser::parse_dyldinfo_generic_bind function of LIEF v0.12.1 allows attackers to cause a Denial of Service (DoS) via a crafted MachO file.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41945	super-xray is a vulnerability scanner (xray) GUI launcher. In version 0.1-beta, the URL is not filtered and directly spliced into the command, resulting in a possible RCE vulnerability. Users should upgrade to super-xray 0.2-beta.	6.5	More Details
CVE-2022-41791	Auth. (subscriber+) CSV Injection vulnerability in ProfileGrid plugin <= 5.1.6 on WordPress.	6.5	More Details
CVE-2022-4096	Server-Side Request Forgery (SSRF) in GitHub repository appsmithorg/appsmith prior to 1.8.2.	6.5	More Details
CVE-2022-41952	Synapse before 1.52.0 with URL preview functionality enabled will attempt to generate URL previews for media stream URLs without properly limiting connection time. Connections will only be terminated after `max_spider_size` (default: 10M) bytes have been downloaded, which can in some cases lead to long-lived connections towards the streaming media server (for instance, Icecast). This can cause excessive traffic and connections toward such servers if their stream URL is, for example, posted to a large room with many Synapse instances with URL preview enabled. Version 1.52.0 implements a timeout mechanism which will terminate URL preview connections after 30 seconds. Since generating URL previews for media streams is not supported and always fails, 1.53.0 additionally implements an allow list for content types for which Synapse will even attempt to generate a URL preview. Upgrade to 1.53.0 to fully resolve the issue. As a workaround, turn off URL preview functionality by setting `url_preview_enabled: false` in the Synapse configuration file.	6.5	More Details
CVE-2022-41950	super-xray is the GUI alternative for vulnerability scanning tool xray. In 0.2-beta, a privilege escalation vulnerability was discovered. This caused inaccurate default xray permissions. Note: this vulnerability only affects Linux and Mac OS systems. Users should upgrade to super-xray 0.3-beta.	6.4	More Details
CVE-2022-41609	Auth. (subscriber+) Server-Side Request Forgery (SSRF) vulnerability in Better Messages plugin 1.9.10.68 on WordPress.	6.4	More Details
CVE-2022-4022	The SVG Support plugin for WordPress defaults to insecure settings in version 2.5 and 2.5.1. SVG files containing malicious javascript are not sanitized. While version 2.5 adds the ability to sanitize image as they are uploaded, the plugin defaults to disable sanitization and does not restrict SVG upload to only administrators. This allows authenticated attackers, with author-level privileges and higher, to upload malicious SVG files that can be embedded in posts and pages by higher privileged users. Additionally, the embedded JavaScript is also triggered on visiting the image URL, which allows an attacker to execute malicious code in browsers visiting that URL.	6.4	More Details
CVE-2022-45077	Auth. (subscriber+) PHP Object Injection vulnerability in Betheme theme <= 26.5.1.4 on WordPress.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41920	Lancet is a general utility library for the go programming language. Affected versions are subject to a ZipSlip issue when using the fileutil package to unzip files. This issue has been addressed and a fix will be included in versions 2.1.10 and 1.3.4. Users are advised to upgrade. There are no known workarounds for this issue.	6.3	More Details
CVE-2022-4012	A vulnerability classified as critical has been found in Hospital Management Center. Affected is an unknown function of the file patient-info.php. The manipulation of the argument pt_id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-213786 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-4051	A vulnerability has been found in Hostel Searching Project and classified as critical. This vulnerability affects unknown code of the file view-property.php. The manipulation of the argument property_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-213844.	6.3	More Details
CVE-2022-45069	Auth. (contributor+) Privilege Escalation vulnerability in Crowdsignal Dashboard plugin <= 3.0.9 on WordPress.	6.3	More Details
CVE-2022-44787	An issue was discovered in Appalti & Contratti 9.12.2. The web applications are vulnerable to a Reflected Cross-Site Scripting issue. The idPagina parameter is reflected inside the server response without any HTML encoding, resulting in XSS when the victim moves the mouse pointer inside the page. As an example, the onmouseenter attribute is not sanitized.	6.1	More Details
CVE-2022-43263	A cross-site scripting (XSS) vulnerability in Arobas Music Guitar Pro for iPad and iPhone before v1.10.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload inserted into the name of an uploaded file.	6.1	More Details
CVE-2022-41615	Cross-Site Scripting (XSS) via Cross-Site Request Forgery (CSRF) vulnerability in Store Locator plugin <= 1.4.5 on WordPress.	6.1	More Details
CVE-2022-31616	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to denial of service, or information disclosure.	6.1	More Details
CVE-2022-36357	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Webpsilon ULTIMATE TABLES plugin <= 1.6.5 versions.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39181	GLPI - Reports plugin for GLPI Reflected Cross-Site-Scripting (RXSS). Type 1: Reflected XSS (or Non-Persistent) - The server reads data directly from the HTTP request and reflects it back in the HTTP response. Reflected XSS exploits occur when an attacker causes a victim to supply dangerous content to a vulnerable web application, which is then reflected back to the victim and executed by the web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or emailed directly to the victim. URLs constructed in this manner constitute the core of many phishing schemes, whereby an attacker convinces a victim to visit a URL that refers to a vulnerable site. After the site reflects the attacker's content back to the victim, the content is executed by the victim's browser.	6.1	More Details
CVE-2022-41132	Unauthenticated Plugin Settings Change Leading To Stored XSS Vulnerability in Ezoic plugin <= 2.8.8 on WordPress.	6.1	More Details
CVE-2022-38462	Silverstripe silverstripe/framework through 4.11 is vulnerable to XSS by carefully crafting a return URL on a /dev/build or /Security/login request.	6.1	More Details
CVE-2022-43332	A cross-site scripting (XSS) vulnerability in Wondercms v3.3.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Site title field of the Configuration Panel.	6.1	More Details
CVE-2021-31739	The SEPPmail solution is vulnerable to a Cross-Site Scripting vulnerability (XSS), because user input is not correctly encoded in HTML attributes when returned by the server.SEPPmail 11.1.10 allows XSS via a recipient address.	6.1	More Details
CVE-2021-22141	An open redirect flaw was found in Kibana versions before 7.13.0 and 6.8.16. If a logged in user visits a maliciously crafted URL, it could result in Kibana redirecting the user to an arbitrary website.	6.1	More Details
CVE-2022-44002	An issue was discovered in BACKCLICK Professional 5.9.63. Due to insufficient output encoding of user-supplied data, the web application is vulnerable to cross-site scripting (XSS) at various locations.	6.1	More Details
CVE-2022-0421	The Five Star Restaurant Reservations WordPress plugin before 2.4.12 does not have authorisation when changing whether a payment was successful or failed, allowing unauthenticated users to change the payment status of arbitrary bookings. Furthermore, due to the lack of sanitisation and escaping, attackers could perform Cross-Site Scripting attacks against a logged in admin viewing the failed payments	6.1	More Details
CVE-2022-3516	Cross-site Scripting (XSS) - Stored in GitHub repository librenms/librenms prior to 22.10.0.	6.1	More Details
CVE-2022-43708	MyBB 1.8.31 has a (issue 2 of 2) cross-site scripting (XSS) vulnerabilities in the post Attachments interface allow attackers to inject HTML by persuading the user to upload a file with specially crafted name	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42187	Hustoj 22.09.22 has a XSS Vulnerability in /admin/problem_judge.php.	6.1	More Details
CVE-2022-3561	Cross-site Scripting (XSS) - Generic in GitHub repository librenms/librenms prior to 22.10.0.	6.1	More Details
CVE-2022-43707	MyBB 1.8.31 has a Cross-site scripting (XSS) vulnerability in the visual MyCode editor (SCEditor) allows remote attackers to inject HTML via user input or stored data	6.1	More Details
CVE-2022-41939	knative.dev/func is is a client library and CLI enabling the development and deployment of Kubernetes functions. Developers using a malicious or compromised third-party buildpack could expose their registry credentials or local docker socket to a malicious `lifecycle` container. This issues has been patched in PR #1442, and is part of release 1.8.1. This issue only affects users who are using function buildpacks from third-parties; pinning the builder image to a specific content-hash with a valid `lifecycle` image will also mitigate the attack.	6.1	More Details
CVE-2022-43142	A cross-site scripting (XSS) vulnerability in the add-fee.php component of Password Storage Application v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the cmddept parameter.	6.1	More Details
CVE-2022-38075	Cross-Site Request Forgery (CSRF) vulnerability leading to Stored Cross-Site Scripting (XSS) in Mantenimiento web plugin <= 0.13 on WordPress.	6.1	More Details
CVE-2022-2791	Emerson Electric's Proficy Machine Edition Version 9.00 and prior is vulnerable to CWE-434 Unrestricted Upload of File with Dangerous Type, and will upload any file written into the PLC logic folder to the connected PLC.	5.9	More Details
CVE-2022-39199	immudb is a database with built-in cryptographic proof and verification. immudb client SDKs use server's UUID to distinguish between different server instance so that the client can connect to different immudb instances and keep the state for multiple servers. SDK does not validate this uuid and can accept any value reported by the server. A malicious server can change the reported UUID tricking the client to treat it as a different server thus accepting a state completely irrelevant to the one previously retrieved from the server. This issue has been patched in version 1.4.1. As a workaround, when initializing an immudb client object a custom state handler can be used to store the state. Providing custom implementation that ignores the server UUID can be used to ensure that even if the server changes the UUID, client will still consider it to be the same server.	5.8	More Details
CVE-2022-24939	A malformed packet containing an invalid destination address, causes a stack overflow in the Ember ZNet stack. This causes an assert which leads to a reset, immediately clearing the error.	5.7	More Details
CVE-2022-39397	aliyun-oss-client is a rust client for Alibaba Cloud OSS. Users of this library will be affected, the incoming secret will be disclosed unintentionally. This issue has been patched in version 0.8.1.	5.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4065	A vulnerability was found in cbeust testng 7.5.0/7.6.0/7.6.1/7.7.0. It has been declared as critical. Affected by this vulnerability is the function testngXmlExistsInJar of the file testng-core/src/main/java/org/testng/JarFileUtils.java of the component XML File Parser. The manipulation leads to path traversal. The attack can be launched remotely. Upgrading to version 7.5.1 and 7.7.1 is able to address this issue. The patch is named 9150736cd2c123a6a3b60e6193630859f9f0422b. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-214027.	5.5	More Details
CVE-2022-45473	In drachtio-server 0.8.18, /var/log/drachtio has mode 0777 and drachtio.log has mode 0666.	5.5	More Details
CVE-2022-31615	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service.	5.5	More Details
CVE-2022-45146	An issue was discovered in the FIPS Java API of Bouncy Castle BC-FJA before 1.0.2.4. Changes to the JVM garbage collector in Java 13 and later trigger an issue in the BC-FJA FIPS modules where it is possible for temporary keys used by the module to be zeroed out while still in use by the module, resulting in errors or potential information loss. NOTE: FIPS compliant users are unaffected because the FIPS certification is only for Java 7, 8, and 11.	5.5	More Details
CVE-2022-39320	FreeRDP is a free remote desktop protocol library and clients. Affected versions of FreeRDP may attempt integer addition on too narrow types leads to allocation of a buffer too small holding the data written. A malicious server can trick a FreeRDP based client to read out of bound data and send it back to the server. This issue has been addressed in version 2.9.0 and all users are advised to upgrade. Users unable to upgrade should not use the `/usb` redirection switch.	5.5	More Details
CVE-2022-40954	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Apache Airflow Spark Provider, Apache Airflow allows an attacker to read arbtrary files in the task execution context, without write access to DAG files. This issue affects Spark Provider versions prior to 4.0.0. It also impacts any Apache Airflow versions prior to 2.3.0 in case Spark Provider is installed (Spark Provider 4.0.0 can only be installed for Airflow 2.3.0+). Note that you need to manually install the Spark Provider version 4.0.0 in order to get rid of the vulnerability on top of Airflow 2.3.0+ version that has lower version of the Spark Provider installed).	5.5	More Details
CVE-2021-33897	A buffer overflow in Synthesia before 10.7.5567, when a non-Latin locale is used, allows user-assisted attackers to cause a denial of service (application crash) via a crafted MIDI file with malformed bytes. This file is mishandled during a deletion attempt. In Synthesia before 10.9, an improper path handling allows local attackers to cause a denial of service (application crash) via a crafted MIDI file with malformed bytes.	5.5	More Details
CVE-2022-42960	EqualWeb Accessibility Widget 2.0.0, 2.0.1, 2.0.2, 2.0.3, 2.0.4, 2.1.10, 3.0.0, 3.0.1, 3.0.2, 4.0.0, and 4.0.1 allows DOM XSS due to improper validation of message events to accessibility.js.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44069	Zenario CMS 9.3.57186 is vulnerable to Cross Site Scripting (XSS) via the Nest library module.	5.4	More Details
CVE-2022-44737	Multiple Cross-Site Request Forgery vulnerabilities in All-In-One Security (AIOS) – Security and Firewall (WordPress plugin) <= 5.1.0 on WordPress.	5.4	More Details
CVE-2022-44073	Zenario CMS 9.3.57186 is vulnerable to Cross Site Scripting (XSS) via svg,Users & Contacts.	5.4	More Details
CVE-2022-44071	Zenario CMS 9.3.57186 is is vulnerable to Cross Site Scripting (XSS) via profile.	5.4	More Details
CVE-2022-44070	Zenario CMS 9.3.57186 is vulnerable to Cross Site Scripting (XSS) via News articles.	5.4	More Details
CVE-2022-39834	A stored XSS vulnerability was discovered in adminweb/ra/viewendentity.jsp in PrimeKey EJBCA through 7.9.0.2. A low-privilege user can store JavaScript in order to exploit a higher-privilege user.	5.4	More Details
CVE-2022-3562	Cross-site Scripting (XSS) - Stored in GitHub repository librenms/librenms prior to 22.10.0.	5.4	More Details
CVE-2022-36432	The Preview functionality in the Amasty Blog Pro 2.10.3 plugin for Magento 2 uses eval unsafely. This allows attackers to perform Cross-site Scripting attacks on admin panel users by manipulating the generated preview application response.	5.4	More Details
CVE-2022-41685	Multiple Cross-Site Request Forgery (CSRF) vulnerabilities in Viszt Péter's Integration for Szamlazz.hu & WooCommerce plugin <= 5.6.3.2 and Csomagpontok és szállítási címkék WooCommerce-hez plugin <= 1.9.0.2 on WordPress.	5.4	More Details
CVE-2022-45073	Cross-Site Request Forgery (CSRF) vulnerability in REST API Authentication plugin <= 2.4.0 on WordPress.	5.4	More Details
CVE-2022-40695	Multiple Cross-Site Scripting (CSRF) vulnerabilities in SEO Redirection Plugin plugin <= 8.9 on WordPress.	5.4	More Details
CVE-2022-42461	Broken Access Control vulnerability in miniOrange's Google Authenticator plugin <= 5.6.1 on WordPress.	5.4	More Details
CVE-2022-41805	Cross-Site Request Forgery (CSRF) vulnerability in Booster for WooCommerce plugin <= 5.6.6 on WordPress.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43117	Sourcecodester Password Storage Application in PHP/OOP and MySQL 1.0 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities via the Name, Username, Description and Site Feature parameters.	5.4	More Details
CVE-2022-40687	Cross-Site Request Forgery (CSRF) vulnerability in Creative Mail plugin <= 1.5.4 on WordPress.	5.4	More Details
CVE-2022-40686	Cross-Site Request Forgery (CSRF) vulnerability in Creative Mail plugin <= 1.5.4 on WordPress.	5.4	More Details
CVE-2022-45375	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in iFeature Slider plugin <= 1.2 on WordPress.	5.4	More Details
CVE-2022-4068	A user is able to enable their own account if it was disabled by an admin while the user still holds a valid session. Moreover, the username is not properly sanitized in the admin user overview. This enables an XSS attack that enables an attacker with a low privilege user to execute arbitrary JavaScript in the context of an admin's account.	5.4	More Details
CVE-2022-45066	Auth. (subscriber+) Broken Access Control vulnerability in WooSwipe WooCommerce Gallery plugin <= 2.0.1 on WordPress.	5.4	More Details
CVE-2022-38146	Silverstripe silverstripe/framework through 4.11 allows XSS (issue 2 of 3).	5.4	More Details
CVE-2021-37936	It was discovered that Kibana was not sanitizing document fields containing HTML snippets. Using this vulnerability, an attacker with the ability to write documents to an elasticsearch index could inject HTML. When the Discover app highlighted a search term containing the HTML, it would be rendered for the user.	5.4	More Details
CVE-2021-36905	Multiple Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerabilities in Quiz And Survey Master plugin <= 7.3.4 on WordPress.	5.4	More Details
CVE-2022-40698	Auth. (subscriber+) Cross-Site Scripting (XSS) vulnerability in Quiz And Survey Master plugin <= 7.3.10 on WordPress.	5.4	More Details
CVE-2022-45071	Cross-Site Request Forgery (CSRF) vulnerability in WPML Multilingual CMS premium plugin <= 4.5.13 on WordPress.	5.4	More Details
CVE-2022-45363	Auth. (subscriber+) Stored Cross-Site Scripting (XSS) in Muffingroup Betheme theme <= 26.6.1 on WordPress.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38461	Broken Access Control vulnerability in WPML Multilingual CMS premium plugin <= 4.5.10 on WordPress allows users with a subscriber or higher user role to change plugin settings (selected language for legacy widgets, the default behavior for media content).	5.4	More Details
CVE-2022-41634	Cross-Site Request Forgery (CSRF) vulnerability in Media Library Folders plugin <= 7.1.1 on WordPress.	5.4	More Details
CVE-2022-4105	A stored XSS in a kiwi Test Plan can run malicious javascript which could be chained with an HTML injection to perform a UI redressing attack (clickjacking) and an HTML injection which disables the use of the history page.	5.4	More Details
CVE-2022-41788	Auth. (subscriber+) Cross-Site Scripting (XSS) vulnerability in Soledad premium theme <= 8.2.5 on WordPress.	5.4	More Details
CVE-2022-38390	Multiple IBM Business Automation Workflow versions are 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: 233978.	5.4	More Details
CVE-2022-42954	Keyfactor EJBCA before 7.10.0 allows XSS.	5.4	More Details
CVE-2022-44740	Multiple Cross-Site Request Forgery (CSRF) vulnerabilities in Creative Mail plugin <= 1.5.4 on WordPress.	5.4	More Details
CVE-2022-4067	Cross-site Scripting (XSS) - Stored in GitHub repository librenms/librenms prior to 22.10.0.	5.4	More Details
CVE-2022-1581	The WP-Polls WordPress plugin before 2.76.0 prioritizes getting a visitor's IP from certain HTTP headers over PHP's REMOTE_ADDR, which makes it possible to bypass IP-based limitations to vote in certain situations.	5.3	More Details
CVE-2022-41936	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. The `modifications` rest endpoint does not filter out entries according to the user's rights. Therefore, information hidden from unauthorized users are exposed though the `modifications` rest endpoint (comments and page names etc). Users should upgrade to XWiki 14.6+, 14.4.3+, or 13.10.8+. Older versions have not been patched. There are no known workarounds.	5.3	More Details
CVE-2022-38755	A vulnerability has been identified in Micro Focus Filr in versions prior to 4.3.1.1. The vulnerability could be exploited to allow a remote unauthenticated attacker to enumerate valid users of the system. Remote unauthenticated user enumeration. This issue affects: Micro Focus Filr versions prior to 4.3.1.1.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3920	HashiCorp Consul and Consul Enterprise 1.13.0 up to 1.13.3 do not filter cluster filtering's imported nodes and services for HTTP or RPC endpoints used by the UI. Fixed in 1.14.0.	5.3	More Details
CVE-2022-45163	An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)	5.3	More Details
CVE-2022-44005	An issue was discovered in BACKCLICK Professional 5.9.63. Due to the use of consecutive IDs in verification links, the newsletter sign-up functionality is vulnerable to the enumeration of subscribers' e-mail addresses. Furthermore, it is possible to subscribe and verify other persons' e-mail addresses to newsletters without their consent.	5.3	More Details
CVE-2022-41839	Broken Access Control vulnerability in WordPress LoginPress plugin <= 1.6.2 on WordPress leading to unauth. changing of Opt-In or Opt-Out tracking settings.	5.3	More Details
CVE-2022-42883	Sensitive Information Disclosure vulnerability discovered by Quiz And Survey Master plugin <= 7.3.10 on WordPress.	5.3	More Details
CVE-2022-41155	Block BYPASS vulnerability in iQ Block Country plugin <= 1.2.18 on WordPress.	5.3	More Details
CVE-2022-39178	Webvendome - webvendome Internal Server IP Disclosure. Send GET Request to the request which is shown in the picture. Internal Server IP and Full path disclosure.	5.3	More Details
CVE-2022-42892	A vulnerability has been identified in syngo Dynamics (All versions < VA40G HF01). syngo Dynamics application server hosts a web service using an operation with improper write access control that could allow directory listing in any folder accessible to the account assigned to the website’s application pool.	5.3	More Details
CVE-2022-3500	A vulnerability was found in keylime. This security issue happens in some circumstances, due to some improperly handled exceptions, there exists the possibility that a rogue agent could create errors on the verifier that stopped attestation attempts for that host leaving it in an attested state but not verifying that anymore.	5.1	More Details
CVE-2022-44634	Auth. (admin+) Arbitrary File Read vulnerability in S2W – Import Shopify to WooCommerce plugin <= 1.1.12 on WordPress.	4.9	More Details
CVE-2022-43709	MyBB 1.8.31 has a SQL injection vulnerability in the Admin CP's Users module allows remote authenticated users to modify the query string via direct user input or stored search filter settings.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40751	IBM UrbanCode Deploy (UCD) 6.2.7.0 through 6.2.7.17, 7.0.0.0 through 7.0.5.12, 7.1.0.0 through 7.1.2.8, and 7.2.0.0 through 7.2.3.1 could allow a user with administrative privileges including "Manage Security" permissions may be able to recover a credential previously saved for performing authenticated LDAP searches. IBM X-Force ID: 236601.	4.9	More Details
CVE-2022-45536	AeroCMS v0.0.1 was discovered to contain a SQL Injection vulnerability via the id parameter at \admin\post_comments.php. This vulnerability allows attackers to access database information.	4.9	More Details
CVE-2022-39383	KubeVela is an open source application delivery platform. Users using the VelaUX APIServer could be affected by this vulnerability. When using Helm Chart as the component delivery method, the request address of the warehouse is not restricted, and there is a blind SSRF vulnerability. Users who're using v1.6, please update the v1.6.1. Users who're using v1.5, please update the v1.5.8. There are no known workarounds for this issue.	4.9	More Details
CVE-2022-45529	AeroCMS v0.0.1 was discovered to contain a SQL Injection vulnerability via the post_category_id parameter at \admin\includes\edit_post.php. This vulnerability allows attackers to access database information.	4.9	More Details
CVE-2022-45535	AeroCMS v0.0.1 was discovered to contain a SQL Injection vulnerability via the edit parameter at \admin\categories.php. This vulnerability allows attackers to access database information.	4.9	More Details
CVE-2022-42985	The ScratchLogin extension through 1.1 for MediaWiki does not escape verification failure messages, which allows users with administrator privileges to perform cross-site scripting (XSS).	4.8	More Details
CVE-2022-41890	TensorFlow is an open source platform for machine learning. If `BCast::ToShape` is given input larger than an `int32`, it will crash, despite being supposed to handle up to an `int64`. An example can be seen in `tf.experimental.numpy.outer` by passing in large input to the input `b`. We have patched the issue in GitHub commit 8310bf8dd188ff780e7fc53245058215a05bdbe5. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.	4.8	More Details
CVE-2022-41891	TensorFlow is an open source platform for machine learning. If `tf.raw_ops.TensorListConcat` is given `element_shape=[]`, it results segmentation fault which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit fc33f3dc4c14051a83eec6535b608abe1d355fde. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41893	TensorFlow is an open source platform for machine learning. If `tf.raw_ops.TensorListResize` is given a nonscalar value for input `size`, it results `CHECK` fail which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 888e34b49009a4e734c27ab0c43b0b5102682c56. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.	4.8	More Details
CVE-2022-41895	TensorFlow is an open source platform for machine learning. If `MirrorPadGrad` is given outsize input `paddings`, TensorFlow will give a heap OOB error. We have patched the issue in GitHub commit 717ca98d8c3bba348ff62281fdf38dcb5ea1ec92. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.	4.8	More Details
CVE-2022-41897	TensorFlow is an open source platform for machine learning. If `FractionMaxPoolGrad` is given outsize inputs `row_pooling_sequence` and `col_pooling_sequence`, TensorFlow will crash. We have patched the issue in GitHub commit d71090c3e5ca325bdf4b02eb236cfb3ee823e927. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.	4.8	More Details
CVE-2022-41888	TensorFlow is an open source platform for machine learning. When running on GPU, `tf.image.generate_bounding_box_proposals` receives a `scores` input that must be of rank 4 but is not checked. We have patched the issue in GitHub commit cf35502463a88ca7185a99daa7031df60b3c1c98. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.	4.8	More Details
CVE-2022-41898	TensorFlow is an open source platform for machine learning. If `SparseFillEmptyRowsGrad` is given empty inputs, TensorFlow will crash. We have patched the issue in GitHub commit af4a6a3c8b95022c351edae94560acc61253a1b8. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.	4.8	More Details
CVE-2022-41899	TensorFlow is an open source platform for machine learning. Inputs `dense_features` or `example_state_data` not of rank 2 will trigger a `CHECK` fail in `SdcaOptimizer`. We have patched the issue in GitHub commit 80ff197d03db2a70c6a111f97dcdacad1b0babfa. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.	4.8	More Details
CVE-2022-41901	TensorFlow is an open source platform for machine learning. An input `sparse_matrix` that is not a matrix with a shape with rank 0 will trigger a `CHECK` fail in `tf.raw_ops.SparseMatrixNNZ`. We have patched the issue in GitHub commit f856d02e5322821aad155dad9b3acab1e9f5d693. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40470	Phpgurukul Blood Donor Management System 1.0 allows Cross Site Scripting via Add Blood Group Name Feature.	4.8	More Details
CVE-2022-41907	TensorFlow is an open source platform for machine learning. When `tf.raw_ops.ResizeNearestNeighborGrad` is given a large `size` input, it overflows. We have patched the issue in GitHub commit 00c821af032ba9e5f5fa3fe14690c8d28a657624. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.	4.8	More Details
CVE-2022-41908	TensorFlow is an open source platform for machine learning. An input `token` that is not a UTF-8 bytestring will trigger a `CHECK` fail in `tf.raw_ops.PyFunc`. We have patched the issue in GitHub commit 9f03a9d3bafe902c1e6beb105b2f24172f238645. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.	4.8	More Details
CVE-2022-41889	TensorFlow is an open source platform for machine learning. If a list of quantized tensors is assigned to an attribute, the pywrap code fails to parse the tensor and returns a `nullptr`, which is not caught. An example can be seen in `tf.compat.v1.extract_volume_patches` by passing in quantized tensors as input `ksizes`. We have patched the issue in GitHub commit e9e95553e5411834d215e6770c81a83a3d0866ce. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.	4.8	More Details
CVE-2022-41887	TensorFlow is an open source platform for machine learning. `tf.keras.losses.poisson` receives a `y_pred` and `y_true` that are passed through `functor::mul` in `BinaryOp`. If the resulting dimensions overflow an `int32`, TensorFlow will crash due to a size mismatch during broadcast assignment. We have patched the issue in GitHub commit c5b30379ba87cbe774b08ac50c1f6d36df4ebb7c. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1 and 2.9.3, as these are also affected and still in supported range. However, we will not cherrypick this commit into TensorFlow 2.8.x, as it depends on Eigen behavior that changed between 2.8 and 2.9.	4.8	More Details
CVE-2022-42094	Backdrop CMS version 1.23.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the 'Card' content.	4.8	More Details
CVE-2022-39316	FreeRDP is a free remote desktop protocol library and clients. In affected versions there is an out of bound read in ZGFX decoder component of FreeRDP. A malicious server can trick a FreeRDP based client to read out of bound data and try to decode it likely resulting in a crash. This issue has been addressed in the 2.9.0 release. Users are advised to upgrade.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41886	TensorFlow is an open source platform for machine learning. When `tf.raw_ops.ImageProjectiveTransformV2` is given a large output shape, it overflows. We have patched the issue in GitHub commit 8faa6ea692985dbe6ce10e1a3168e0bd60a723ba. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.	4.8	More Details
CVE-2022-42096	Backdrop CMS version 1.23.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability via Post content.	4.8	More Details
CVE-2022-41885	TensorFlow is an open source platform for machine learning. When `tf.raw_ops.FusedResizeAndPadConv2D` is given a large tensor shape, it overflows. We have patched the issue in GitHub commit d66e1d568275e6a2947de97dca7a102a211e01ce. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.	4.8	More Details
CVE-2022-41884	TensorFlow is an open source platform for machine learning. If a numpy array is created with a shape such that one element is zero and the others sum to a large number, an error will be raised. We have patched the issue in GitHub commit 2b56169c16e375c521a3bc8ea658811cc0793784. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.	4.8	More Details
CVE-2022-41911	TensorFlow is an open source platform for machine learning. When printing a tensor, we get it's data as a `const char*` array (since that's the underlying storage) and then we typecast it to the element type. However, conversions from `char` to `bool` are undefined if the `char` is not `0` or `1`, so sanitizers/fuzzers will crash. The issue has been patched in GitHub commit `1be74370327`. The fix will be included in TensorFlow 2.11.0. We will also cherrypick this commit on TensorFlow 2.10.1, TensorFlow 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.	4.8	More Details
CVE-2022-43463	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Custom Product Tabs for WooCommerce plugin <= 1.7.9 on WordPress.	4.8	More Details
CVE-2022-41445	A cross-site scripting (XSS) vulnerability in Record Management System using CodeIgniter 1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Add Subject page.	4.8	More Details
CVE-2022-44736	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Chameleon plugin <= 1.4.3 on WordPress.	4.8	More Details
CVE-2022-44591	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Anthologize plugin <= 0.8.0 on WordPress.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41315	Auth. Stored Cross-Site Scripting (XSS) vulnerability in Ezoic plugin <= 2.8.8 on WordPress.	4.8	More Details
CVE-2022-40694	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in News Announcement Scroll plugin <= 8.8.8 on WordPress.	4.8	More Details
CVE-2022-39318	FreeRDP is a free remote desktop protocol library and clients. Affected versions of FreeRDP are missing input validation in `urbdrc` channel. A malicious server can trick a FreeRDP based client to crash with division by zero. This issue has been addressed in version 2.9.0. All users are advised to upgrade. Users unable to upgrade should not use the `/usb` redirection switch.	4.8	More Details
CVE-2022-42097	Backdrop CMS version 1.23.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability via 'Comment.' .	4.8	More Details
CVE-2022-41909	TensorFlow is an open source platform for machine learning. An input `encoded` that is not a valid `CompositeTensorVariant` tensor will trigger a segfault in `tf.raw_ops.CompositeTensorVariantToComponents`. We have patched the issue in GitHub commits bf594d08d377dc6a3354d9fdb494b32d45f91971 and 660ce5a89eb6766834bdc303d2ab3902aef99d3d. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.	4.8	More Details
CVE-2022-4069	Cross-site Scripting (XSS) - Generic in GitHub repository librenms/librenms prior to 22.10.0.	4.8	More Details
CVE-2022-41896	TensorFlow is an open source platform for machine learning. If `ThreadUnsafeUnigramCandidateSampler` is given input `filterbank_channel_count` greater than the allowed max size, TensorFlow will crash. We have patched the issue in GitHub commit 39ec7eaf1428e90c37787e5b3fbd68ebd3c48860. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.	4.8	More Details
CVE-2022-3753	The Evaluate WordPress plugin through 1.0 does not sanitize and escapes some of its settings, which could allow high-privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example, in multisite setup).	4.8	More Details
CVE-2022-3618	The Spacer WordPress plugin before 3.0.7 does not sanitize and escapes some of its settings, which could allow high-privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example, in multisite setup).	4.8	More Details
CVE-2022-45017	A cross-site scripting (XSS) vulnerability in the Overview Page settings module of WBCE CMS v1.5.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Post Loop field.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45016	A cross-site scripting (XSS) vulnerability in the Search Settings module of WBCE CMS v1.5.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Footer field.	4.8	More Details
CVE-2022-45015	A cross-site scripting (XSS) vulnerability in the Search Settings module of WBCE CMS v1.5.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Results Footer field.	4.8	More Details
CVE-2022-45014	A cross-site scripting (XSS) vulnerability in the Search Settings module of WBCE CMS v1.5.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Results Header field.	4.8	More Details
CVE-2022-45013	A cross-site scripting (XSS) vulnerability in the Show Advanced Option module of WBCE CMS v1.5.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Section Header field.	4.8	More Details
CVE-2022-45012	A cross-site scripting (XSS) vulnerability in the Modify Page module of WBCE CMS v1.5.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Source field.	4.8	More Details
CVE-2022-3690	The Popup Maker WordPress plugin before 1.16.11 does not sanitise and escape some of its Popup options, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks, which could be used against admins	4.8	More Details
CVE-2022-40963	Multiple Auth. (author+) Stored Cross-Site Scripting (XSS) vulnerabilities in WP Page Builder plugin <= 1.2.6 on WordPress.	4.8	More Details
CVE-2022-41643	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Accessibility plugin <= 1.0.3 on WordPress.	4.8	More Details
CVE-2022-3750	The has a CSRF vulnerability that allows the deletion of a post without using a nonce or prompting for confirmation.	4.7	More Details
CVE-2022-4015	A vulnerability, which was classified as critical, was found in Sports Club Management System 119. This affects an unknown part of the file admin/make_payments.php. The manipulation of the argument m_id/plan leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-213789 was assigned to this vulnerability.	4.7	More Details
CVE-2022-4052	A vulnerability was found in Student Attendance Management System and classified as critical. This issue affects some unknown processing of the file /Admin/createClass.php. The manipulation of the argument Id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-213845 was assigned to this vulnerability.	4.7	More Details
CVE-2022-43673	Wire through 3.22.3993 on Windows advertises deletion of sent messages; nonetheless, all messages can be retrieved (for a limited period of time) from the AppData\Roaming\Wire\IndexedDB\https_app.wire.com_0.indexeddb.leveldb database.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41877	FreeRDP is a free remote desktop protocol library and clients. Affected versions of FreeRDP are missing input length validation in `drive` channel. A malicious server can trick a FreeRDP based client to read out of bound data and send it back to the server. This issue has been addressed in version 2.9.0 and all users are advised to upgrade. Users unable to upgrade should not use the drive redirection channel - command line options `/drive`, `+drives` or `+home-drive`.	4.6	More Details
CVE-2022-39317	FreeRDP is a free remote desktop protocol library and clients. Affected versions of FreeRDP are missing a range check for input offset index in ZGFX decoder. A malicious server can trick a FreeRDP based client to read out of bound data and try to decode it. This issue has been addressed in version 2.9.0. There are no known workarounds for this issue.	4.6	More Details
CVE-2022-39319	FreeRDP is a free remote desktop protocol library and clients. Affected versions of FreeRDP are missing input length validation in the `urbdrc` channel. A malicious server can trick a FreeRDP based client to read out of bound data and send it back to the server. This issue has been addressed in version 2.9.0 and all users are advised to upgrade. Users unable to upgrade should not use the `/usb` redirection switch.	4.6	More Details
CVE-2022-34667	NVIDIA CUDA Toolkit SDK contains a stack-based buffer overflow vulnerability in cuobjdump, where an unprivileged remote attacker could exploit this buffer overflow condition by persuading a local user to download a specially crafted corrupted file and execute cuobjdump against it locally, which may lead to a limited denial of service and some loss of data integrity for the local user.	4.4	More Details
CVE-2021-31608	Proofpoint Enterprise Protection before 18.8.0 allows a Bypass of a Security Control.	4.3	More Details
CVE-2022-45072	Cross-Site Request Forgery (CSRF) vulnerability in WPML Multilingual CMS premium plugin <= 4.5.13 on WordPress.	4.3	More Details
CVE-2022-4018	Missing Authentication for Critical Function in GitHub repository ikus060/rdiffweb prior to 2.5.0a6.	4.3	More Details
CVE-2022-4014	A vulnerability, which was classified as problematic, has been found in FeehiCMS. Affected by this issue is some unknown functionality of the component Post My Comment Tab. The manipulation leads to cross-site request forgery. The attack may be launched remotely. The identifier of this vulnerability is VDB-213788.	4.3	More Details
CVE-2022-4013	A vulnerability classified as problematic was found in Hospital Management Center. Affected by this vulnerability is an unknown functionality of the file appointment.php. The manipulation leads to cross-site request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-213787.	4.3	More Details
CVE-2022-40130	Auth. (subscriber+) Race Condition vulnerability in WP-Polls plugin <= 2.76.0 on WordPress.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41917	OpenSearch is a community-driven, open source fork of Elasticsearch and Kibana. OpenSearch allows users to specify a local file when defining text analyzers to process data for text analysis. An issue in the implementation of this feature allows certain specially crafted queries to return a response containing the first line of text from arbitrary files. The list of potentially impacted files is limited to text files with read permissions allowed in the Java Security Manager policy configuration. OpenSearch version 1.3.7 and 2.4.0 contain a fix for this issue. Users are advised to upgrade. There are no known workarounds for this issue.	4.3	More Details
CVE-2022-3336	The Event Monster WordPress plugin before 1.2.0 does not have CSRF check when deleting visitors, which could allow attackers to make logged in admin delete arbitrary visitors via a CSRF attack	4.3	More Details
CVE-2022-40216	Auth. (subscriber+) Messaging Block Bypass vulnerability in Better Messages plugin <= 1.9.10.69 on WordPress.	4.3	More Details
CVE-2022-41655	Auth. (subscriber+) Sensitive Data Exposure vulnerability in Phone Orders for WooCommerce plugin <= 3.7.1 on WordPress.	4.3	More Details
CVE-2022-38974	Broken Access Control vulnerability in WPML Multilingual CMS premium plugin <= 4.5.10 on WordPress allows users with subscriber or higher user roles to change the status of the translation jobs.	4.3	More Details
CVE-2022-41692	Missing Authorization vulnerability in Appointment Hour Booking plugin <= 1.3.71 on WordPress.	4.3	More Details
CVE-2022-45369	Auth. (subscriber+) Broken Access Control vulnerability in Plugin for Google Reviews plugin <= 2.2.2 on WordPress.	4.3	More Details
CVE-2022-43492	Auth. (subscriber+) Insecure Direct Object References (IDOR) vulnerability in Comments – wpDiscuz plugin 7.4.2 on WordPress.	4.3	More Details
CVE-2022-43482	Missing Authorization vulnerability in Appointment Booking Calendar plugin <= 1.3.69 on WordPress.	4.3	More Details
CVE-2022-41919	Fastify is a web framework with minimal overhead and plugin architecture. The attacker can use the incorrect `Content-Type` to bypass the `Pre-Flight` checking of `fetch`. `fetch()` requests with Content-Type's essence as "application/x-www-form-urlencoded", "multipart/form-data", or "text/plain", could potentially be used to invoke routes that only accepts `application/json` content type, thus bypassing any CORS protection, and therefore they could lead to a Cross-Site Request Forgery attack. This issue has been patched in version 4.10.2 and 3.29.4. As a workaround, implement Cross-Site Request Forgery protection using `@fastify/csrf'.	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34354	IBM Sterling Partner Engagement Manager 2.0 allows encrypted storage of client data to be stored locally which can be read by another user on the system. IBM X-Force ID: 230424.	4.0	More Details
CVE-2022-41914	Zulip is an open-source team collaboration tool. For organizations with System for Cross-domain Identity Management(SCIM) account management enabled, Zulip Server 5.0 through 5.6 checked the SCIM bearer token using a comparator that did not run in constant time. Therefore, it might theoretically be possible for an attacker to infer the value of the token by performing a sophisticated timing analysis on a large number of failing requests. If successful, this would allow the attacker to impersonate the SCIM client for its abilities to read and update user accounts in the Zulip organization. Organizations where SCIM account management has not been enabled are not affected.	3.7	More Details
CVE-2022-41618	Unauthenticated Error Log Disclosure vulnerability in Media Library Assistant plugin <= 3.00 on WordPress.	3.7	More Details
CVE-2022-40228	IBM DataPower Gateway 10.0.3.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.9, 2018.4.1.0 through 2018.4.1.22, and 10.5.0.0 through 10.5.0.2 does not invalidate session after a password change which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 235527.	3.7	More Details
CVE-2022-45471	In JetBrains Hub before 2022.3.15181 Throttling was missed when sending emails to a particular email address	3.5	More Details
CVE-2022-4066	A vulnerability was found in davidmoreno onion. It has been rated as problematic. Affected by this issue is the function onion_response_flush of the file src/onion/response.c of the component Log Handler. The manipulation leads to allocation of resources. The name of the patch is de8ea938342b36c28024fd8393ebc27b8442a161. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-214028.	3.5	More Details
CVE-2022-45082	Multiple Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerabilities in Accordions plugin <= 2.0.3 on WordPress via &addons-style-name and &accordions_or_faqs_license_key.	3.4	More Details
CVE-2022-42903	Zoho ManageEngine SupportCenter Plus through 11024 allows low-privileged users to view the organization users list.	3.3	More Details
CVE-2022-28766	Windows 32-bit versions of the Zoom Client for Meetings before 5.12.6 and Zoom Rooms for Conference Room before version 5.12.6 are susceptible to a DLL injection vulnerability. A local low-privileged user could exploit this vulnerability to run arbitrary code in the context of the Zoom client.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4064	A vulnerability was found in Dalli. It has been classified as problematic. Affected is the function self.meta_set of the file lib/dalli/protocol/meta/request_formatter.rb of the component Meta Protocol Handler. The manipulation leads to injection. The exploit has been disclosed to the public and may be used. The name of the patch is 48d594dae55934476fec61789e7a7c3700e0f50d. It is recommended to apply a patch to fix this issue. VDB-214026 is the identifier assigned to this vulnerability.	3.1	More Details
CVE-2022-39347	FreeRDP is a free remote desktop protocol library and clients. Affected versions of FreeRDP are missing path canonicalization and base path check for `drive` channel. A malicious server can trick a FreeRDP based client to read files outside the shared directory. This issue has been addressed in version 2.9.0 and all users are advised to upgrade. Users unable to upgrade should not use the `/drive`, `/drives` or `+home-drive` redirection switch.	2.6	More Details
CVE-2022-4087	A vulnerability was found in iPXE. It has been declared as problematic. This vulnerability affects the function tls_new_ciphertext of the file src/net/tls.c of the component TLS. The manipulation of the argument pad_len leads to information exposure through discrepancy. The name of the patch is 186306d6199096b7a7c4b4574d4be8cdb8426729. It is recommended to apply a patch to fix this issue. VDB-214054 is the identifier assigned to this vulnerability.	2.6	More Details
CVE-2022-4053	A vulnerability was found in Student Attendance Management System. It has been classified as problematic. Affected is an unknown function of the file createClass.php. The manipulation of the argument className leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-213846 is the identifier assigned to this vulnerability.	2.4	More Details
CVE-2022-4072	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-4073	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-4071	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-44577	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-4086	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-4074	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4083	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-4075	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-4082	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-4076	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-4084	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-4077	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-4078	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-4079	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-4080	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-4081	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-4085	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details