SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 06 July 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-2022-2185	A critical issue has been discovered in GitLab affecting all versions starting from 14.0 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 where an authenticated user authorized to import projects could import a maliciously crafted project leading to remote code execution.	9.9	More Details
CVE-2022-32532	Apache Shiro before 1.9.1, A RegexRequestMatcher can be misconfigured to be bypassed on some servlet containers. Applications using RegExPatternMatcher with `.` in the regular expression are possibly vulnerable to an authorization bypass.	9.8	More Details
CVE-2022-33107	ThinkPHP v6.0.12 was discovered to contain a deserialization vulnerability via the component vendor\league\flysystem-cached-adapter\src\Storage\AbstractCache.php. This vulnerability allows attackers to execute arbitrary code via a crafted payload.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2274	The OpenSSL 3.0.4 release introduced a serious bug in the RSA implementation for X86_64 CPUs supporting the AVX512IFMA instructions. This issue makes the RSA implementation with 2048 bit private keys incorrect on such machines and memory corruption will happen during the computation. As a consequence of the memory corruption an attacker may be able to trigger a remote code execution on the machine performing the computation. SSL/TLS servers or other servers using 2048 bit RSA private keys running on machines supporting AVX512IFMA instructions of the X86_64 architecture are affected by this issue.	9.8	More Details
CVE-2022-31604	NVFLARE, versions prior to 2.1.2, contains a vulnerability in its PKI implementation module, where The CA credentials are transported via pickle and no safe deserialization. The deserialization of Untrusted Data may allow an unprivileged network attacker to cause Remote Code Execution, Denial Of Service, and Impact to both Confidentiality and Integrity.	9.8	More Details
CVE-2022-31605	NVFLARE, versions prior to 2.1.2, contains a vulnerability in its utils module, where YAML files are loaded via yaml.load() instead of yaml.safe_load(). The deserialization of Untrusted Data, may allow an unprivileged network attacker to cause Remote Code Execution, Denial Of Service, and Impact to both Confidentiality and Integrity.	9.8	More Details
CVE-2022-32032	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow via the deviceList parameter in the function formAddMacfilterRule.	9.8	More Details
CVE-2022-31943	MCMS v5.2.8 was discovered to contain an arbitrary file upload vulnerability.	9.8	More Details
CVE-2022-32093	Hospital Management System v1.0 was discovered to contain a SQL injection vulnerability via the loginid parameter at adminlogin.php.	9.8	More Details
CVE-2022-32094	Hospital Management System v1.0 was discovered to contain a SQL injection vulnerability via the loginid parameter at doctorlogin.php.	9.8	More Details
CVE-2022-32095	Hospital Management System v1.0 was discovered to contain a SQL injection vulnerability via the editid parameter at orders.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32324	PDFAlto v0.4 was discovered to contain a heap buffer overflow via the component /pdfalto/src/pdfalto.cc.	9.8	More Details
CVE-2022-34913	md2roff 1.7 has a stack-based buffer overflow via a Markdown file containing a large number of consecutive characters to be processed. NOTE: the vendor's position is that the product is not intended for untrusted input	9.8	More Details
CVE-2022-33171	The findOne function in TypeORM before 0.3.0 can either be supplied with a string or a FindOneOptions object. When input to the function is a user-controlled parsed JSON object, supplying a crafted FindOneOptions instead of an id string leads to SQL injection. NOTE: the vendor's position is that the user's application is responsible for input validation	9.8	More Details
CVE-2022-34265	An issue was discovered in Django 3.2 before 3.2.14 and 4.0 before 4.0.6. The Trunc() and Extract() database functions are subject to SQL injection if untrusted data is used as a kind/lookup_name value. Applications that constrain the lookup name and kind choice to a known safe list are unaffected.	9.8	More Details
CVE-2022-31836	The leafInfo.match() function in Beego v2.0.3 and below uses path.join() to deal with wildcardvalues which can lead to cross directory risk.	9.8	More Details
CVE-2022-2321	Improper Restriction of Excessive Authentication Attempts in GitHub repository heroiclabs/nakama prior to 3.13.0. This results in login brute-force attacks.	9.8	More Details
CVE-2022-31856	Newsletter Module v3.x was discovered to contain a SQL injection vulnerability via the zemez_newsletter_email parameter at /index.php.	9.8	More Details
CVE-2022-32310	An access control issue in Ingredient Stock Management System v1.0 allows attackers to take over user accounts via a crafted POST request to /isms/classes/Users.php.	9.8	More Details
CVE-2022-32311	Ingredient Stock Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /isms/admin/stocks/view_stock.php.	9.8	More Details
CVE-2022-32413	An arbitrary file upload vulnerability in Dice v4.2.0 allows attackers to execute arbitrary code via a crafted file.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32295	On Ampere Altra and AltraMax devices before SRP 1.09, the Altra reference design of UEFI accesses allows insecure access to SPI-NOR by the OS/hypervisor component.	9.8	More Details
CVE-2021-32428	SQL Injection vulnerability in viaviwebtech Android EBook App (Books App, PDF, ePub, Online Book Reading, Download Books) 10 via the author_id parameter to api.php.	9.8	More Details
CVE-2014-0156	Awesome spawn contains OS command injection vulnerability, which allows execution of additional commands passed to Awesome spawn as arguments. If untrusted input was included in command arguments, attacker could use this flaw to execute arbitrary command.	9.8	More Details
CVE-2022-2197	By using a specific credential string, an attacker with network access to the device’s web interface could circumvent the authentication scheme and perform administrative operations.	9.8	More Details
CVE-2021-40597	The firmware of EDIMAX IC-3140W Version 3.11 is hardcoded with Administrator username and password.	9.8	More Details
CVE-2022-34835	In Das U-Boot through 2022.07-rc5, an integer signedness error and resultant stack-based buffer overflow in the "i2c md" command enables the corruption of the return address pointer of the do_i2c_md function.	9.8	More Details
CVE-2021-40643	EyesOfNetwork before 07-07-2021 has a Remote Code Execution vulnerability on the mail options configuration page. In the location of the "sendmail" application in the "cacti" configuration page (by default/usr/sbin/sendmail) it is possible to execute any command, which will be executed when we make a test of the configuration ("send test mail").	9.8	More Details
CVE-2021-40663	deep.assign npm package 0.0.0-alpha.0 is vulnerable to Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution').	9.8	More Details
CVE-2021-41506	Xiaongmai AHB7008T-MH-V2, AHB7804R-ELS, AHB7804R-MH-V2, AHB7808R-MS-V2, AHB7808R-MS, AHB7808T-MS-V2, AHB7804R-LMS, HI3518_50H10L_S39 V4.02.R11.7601.Nat.Onvif.20170420, V4.02.R11.Nat.Onvif.20160422, V4.02.R11.7601.Nat.Onvif.20170424, V4.02.R11.Nat.Onvif.20170327, V4.02.R11.Nat.Onvif.20161205, V4.02.R11.Nat.20170301, V4.02.R12.Nat.OnvifS.20170727 is affected by a backdoor in the macGuarder and dvrHelper binaries of DVR/NVR/IP camera firmware due to static root account credentials in the system.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37778	There is a buffer overflow in gps-sdr-sim v1.0 when parsing long command line parameters, which can lead to DoS or code execution.	9.8	More Details
CVE-2022-22487	An IBM Spectrum Protect storage agent could allow a remote attacker to perform a brute force attack by allowing unlimited attempts to login to the storage agent without locking the administrative ID. A remote attacker could exploit this vulnerability using brute force techniques to gain unauthorized administrative access to both the IBM Spectrum Protect storage agent and the IBM Spectrum Protect Server 8.1.0.000 through 8.1.14 with which it communicates. IBM X-Force ID: 226326.	9.8	More Details
CVE-2013-4144	There is an object injection vulnerability in swfupload plugin for wordpress.	9.8	More Details
CVE-2022-33329	Multiple command injection vulnerabilities exist in the web_server ajax endpoints functionalities of Robustel R1510 3.3.0. A specially-crafted network packets can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger these vulnerabilities.The `/ajax/set_sys_time/` API is affected by a command injection vulnerability.	9.8	More Details
CVE-2022-34972	So Filter Shop v3.x was discovered to contain multiple blind SQL injection vulnerabilities via the att_value_id , manu_value_id , opt_value_id , and subcate_value_id parameters at /index.php?route=extension/module/so_filter_shop_by/filter_data.	9.8	More Details
CVE-2022-32585	A command execution vulnerability exists in the clish art2 functionality of Robustel R1510 3.3.0. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger this vulnerability.	9.8	More Details
CVE-2022-33312	Multiple command injection vulnerabilities exist in the web_server action endpoints functionalities of Robustel R1510 3.3.0. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger these vulnerabilities.The `/action/import_cert_file/` API is affected by command injection vulnerability.	9.8	More Details
CVE-2022-33313	Multiple command injection vulnerabilities exist in the web_server action endpoints functionalities of Robustel R1510 3.3.0. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger these vulnerabilities.The `/action/import_https_cert_file/` API is affected by command injection vulnerability.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33314	Multiple command injection vulnerabilities exist in the web_server action endpoints functionalities of Robustel R1510 3.3.0. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger these vulnerabilities.The `/action/import_sdk_file/` API is affected by command injection vulnerability.	9.8	More Details
CVE-2022-33325	Multiple command injection vulnerabilities exist in the web_server ajax endpoints functionalities of Robustel R1510 3.3.0. A specially-crafted network packets can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger these vulnerabilities.The `/ajax/clear_tools_log/` API is affected by command injection vulnerability.	9.8	More Details
CVE-2022-33326	Multiple command injection vulnerabilities exist in the web_server ajax endpoints functionalities of Robustel R1510 3.3.0. A specially-crafted network packets can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger these vulnerabilities.The `/ajax/config_rollback/` API is affected by a command injection vulnerability.	9.8	More Details
CVE-2022-33327	Multiple command injection vulnerabilities exist in the web_server ajax endpoints functionalities of Robustel R1510 3.3.0. A specially-crafted network packets can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger these vulnerabilities.The `/ajax/remove_sniffer_raw_log/` API is affected by a command injection vulnerability.	9.8	More Details
CVE-2022-33328	Multiple command injection vulnerabilities exist in the web_server ajax endpoints functionalities of Robustel R1510 3.3.0. A specially-crafted network packets can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger these vulnerabilities.The `/ajax/remove/` API is affected by a command injection vulnerability.	9.8	More Details
CVE-2013-4561	In a openshift node, there is a cron job to update mcollective facts that mishandles a temporary file. This may lead to loss of confidentiality and integrity.	9.1	More Details
CVE-2022-2253	A user with administrative privileges in Distributed Data Systems WebHMI 4.1.1.7662 may send OS commands to execute on the host server.	9.1	More Details
CVE-2022-28127	A data removal vulnerability exists in the web_server /action/remove/ API functionality of Robustel R1510 3.3.0. A specially-crafted network request can lead to arbitrary file deletion. An attacker can send a sequence of requests to trigger this vulnerability.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43702	ASUS RT-A88U 3.0.0.4.386_45898 is vulnerable to Cross Site Scripting (XSS). The ASUS router admin panel does not sanitize the WiFI logs correctly, if an attacker was able to change the SSID of the router with a custom payload, they could achieve stored XSS on the device.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-33948	HOME SPOT CUBE2 V102 contains an OS command injection vulnerability due to improper processing of data received from DHCP server. An adjacent attacker may execute an arbitrary OS command on the product if a malicious DHCP server is placed on the WAN side of the product.	8.8	More Details
CVE-2022-32420	College Management System v1.0 was discovered to contain a remote code execution (RCE) vulnerability via /College/admin/teacher.php. This vulnerability is exploited via a crafted PHP file.	8.8	More Details
CVE-2022-22472	IBM Spectrum Protect Plus Container Backup and Restore (10.1.5 through 10.1.10.2 for Kubernetes and 10.1.7 through 10.1.10.2 for Red Hat OpenShift) could allow a remote attacker to bypass IBM Spectrum Protect Plus role based access control restrictions, caused by improper disclosure of session information. By retrieving the logs of a container an attacker could exploit this vulnerability to bypass login security of the IBM Spectrum Protect Plus server and gain unauthorized access based on the permissions of the IBM Spectrum Protect Plus user to the vulnerable Spectrum Protect Plus server software. IBM X-Force ID: 225340.	8.8	More Details
CVE-2021-43116	An Access Control vulnerability exists in Nacos 2.0.3 in the access prompt page; enter username and password, click on login to capture packets and then change the returned package, which lets a malicious user login.	8.8	More Details
CVE-2017-20123	A vulnerability was found in Viscosity 1.6.7. It has been classified as critical. This affects an unknown part of the component DLL Handler. The manipulation leads to untrusted search path. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.6.8 is able to address this issue. It is recommended to upgrade the affected component.	8.8	More Details
CVE-2022-32384	Tenda AC23 v16.03.07.44 was discovered to contain a stack overflow via the security_5g parameter in the function formWifiBasicSet.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31115	opensearch-ruby is a community-driven, open source fork of elasticsearch-ruby. In versions prior to 2.0.1 the ruby `YAML.load` function was used instead of `YAML.safe_load`. As a result opensearch-ruby 2.0.0 and prior can lead to unsafe deserialization using YAML.load if the response is of type YAML. An attacker must be in control of an opensearch server and convince the victim to connect to it in order to exploit this vulnerability. The problem has been patched in opensearch-ruby gem version 2.0.1. Users are advised to upgrade. There are no known workarounds for this issue.	8.8	More Details
CVE-2022-34793	Jenkins Recipe Plugin 1.2 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	8.8	More Details
CVE-2022-2235	Insufficient sanitization in GitLab EE's external issue tracker affecting all versions from 14.5 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows an attacker to perform cross-site scripting when a victim clicks on a maliciously crafted ZenTao link	8.7	More Details
CVE-2022-33639	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	8.3	More Details
CVE-2022-30192	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	8.3	More Details
CVE-2022-33638	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	8.3	More Details
CVE-2022-31599	NVIDIA DGX A100 contains a vulnerability in SBIOS in the Ofbd, where a local user with elevated privileges can cause access to an uninitialized pointer, which may lead to code execution, escalation of privileges, denial of service, and information disclosure. The scope of impact can extend to other components.	8.2	More Details
CVE-2022-28200	NVIDIA DGX A100 contains a vulnerability in SBIOS in the BiosCfgTool, where a local user with elevated privileges can read and write beyond intended bounds in SMRAM, which may lead to code execution, escalation of privileges, denial of service, and information disclosure. The scope of impact can extend to other components.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31112	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. In affected versions parse Server LiveQuery does not remove protected fields in classes, passing them to the client. The LiveQueryController now removes protected fields from the client response. Users are advised to upgrade. Users unable t upgrade should use `Parse.Cloud.afterLiveQueryEvent` to manually remove protected fields.	8.2	More Details
CVE-2022-33208	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller.	8.1	More Details
CVE-2022-25900	All versions of package git-clone are vulnerable to Command Injection due to insecure usage of the --upload-pack feature of git.	8.1	More Details
CVE-2022-34151	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller.	8.1	More Details
CVE-2022-29484	Operation restriction bypass vulnerability in Space of Cybozu Garoon 4.0.0 to 5.9.0 allows a remote authenticated attacker to delete the data of Space.	8.1	More Details
CVE-2021-38941	IBM CloudPak for Multicloud Monitoring 2.0 and 2.3 has a few containers running in privileged mode which is vulnerable to host information leakage or destruction if unauthorized access to these containers could execute arbitrary commands. IBM X-Force ID: 211048.	8.1	More Details
CVE-2022-2230	A Stored Cross-Site Scripting vulnerability in the project settings page in GitLab CE/EE affecting all versions from 14.4 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows an attacker to execute arbitrary JavaScript code in GitLab on a victim's behalf.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34792	A cross-site request forgery (CSRF) vulnerability in Jenkins Recipe Plugin 1.2 and earlier allows attackers to send an HTTP request to an attacker-specified URL and parse the response as XML.	8.0	More Details
CVE-2022-2304	Stack-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.	7.8	More Details
CVE-2022-2288	Out-of-bounds Write in GitHub repository vim/vim prior to 9.0.	7.8	More Details
CVE-2022-2284	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.	7.8	More Details
CVE-2017-20121	A vulnerability was found in Teradici Management Console 2.2.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Database Management. The manipulation leads to improper privilege management. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used.	7.8	More Details
CVE-2022-2285	Integer Overflow or Wraparound in GitHub repository vim/vim prior to 9.0.	7.8	More Details
CVE-2022-2286	Out-of-bounds Read in GitHub repository vim/vim prior to 9.0.	7.8	More Details
CVE-2022-2257	Out-of-bounds Read in GitHub repository vim/vim prior to 9.0.	7.8	More Details
CVE-2022-34918	An issue was discovered in the Linux kernel through 5.18.9. A type confusion bug in nft_set_elem_init (leading to a buffer overflow) could be used by a local attacker to escalate privileges, a different vulnerability than CVE-2022-32250. (The attacker can obtain root access, but must start with an unprivileged user namespace to obtain CAP_NET_ADMIN access.) This can be fixed in nft_setelem_parse_data in net/netfilter/nf_tables_api.c.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33743	network backend may cause Linux netfront to use freed SKBs While adding logic to support XDP (eXpress Data Path), a code label was moved in a way allowing for SKBs having references (pointers) retained for further processing to nevertheless be freed.	7.8	More Details
CVE-2022-2289	Use After Free in GitHub repository vim/vim prior to 9.0.	7.8	More Details
CVE-2022-33037	A binary hijack in Orwell-Dev-Cpp v5.11 allows attackers to execute arbitrary code via a crafted .exe file.	7.8	More Details
CVE-2022-33036	A binary hijack in Embarcadero Dev-CPP v6.3 allows attackers to execute arbitrary code via a crafted .exe file.	7.8	More Details
CVE-2022-33035	XLPD v7.0.0094 and below contains an unquoted service path vulnerability which allows local users to launch processes with elevated privileges.	7.8	More Details
CVE-2017-20112	A vulnerability has been found in IVPN Client 2.6.6120.33863 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation of the argument --up cmd leads to improper privilege management. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. Upgrading to version 2.6.2 is able to address this issue. It is recommended to upgrade the affected component.	7.8	More Details
CVE-2022-2264	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.	7.8	More Details
CVE-2022-33103	Das U-Boot from v2020.10 to v2022.07-rc3 was discovered to contain an out-of-bounds write via the function sqfs_readdir().	7.8	More Details
CVE-2022-25898	The package jsrsasign before 10.5.25 are vulnerable to Improper Verification of Cryptographic Signature when JWS or JWT signature with non Base64URL encoding special characters or number escaped characters may be validated as valid by mistake. Workaround: Validate JWS or JWT signature if it has Base64URL and dot safe string before executing JWS.verify() or JWS.verifyJWT() method.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23725	PingID Windows Login prior to 2.8 does not properly set permissions on the Windows Registry entries used to store sensitive API keys under some circumstances.	7.7	More Details
CVE-2021-41995	A misconfiguration of RSA in PingID Mac Login prior to 1.1 is vulnerable to pre-computed dictionary attacks, leading to an offline MFA bypass.	7.7	More Details
CVE-2022-23718	PingID Windows Login prior to 2.8 uses known vulnerable components that can lead to remote code execution. An attacker capable of achieving a sophisticated man-in-the-middle position, or to compromise Ping Identity web servers, could deliver malicious code that would be executed as SYSTEM by the PingID Windows Login application.	7.6	More Details
CVE-2022-33971	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program.	7.5	More Details
CVE-2022-32551	Zoho ManageEngine ServiceDesk Plus MSP before 10604 allows path traversal (to WEBINF/web.xml from sample/WEB-INF/web.xml or sample/META-INF/web.xml).	7.5	More Details
CVE-2022-32030	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow via the list parameter in the function formSetQosBand.	7.5	More Details
CVE-2022-32041	Tenda M3 V1.0.0.12 was discovered to contain a stack overflow via the function formGetPassengerAnalyseData.	7.5	More Details
CVE-2022-32284	Use of insufficiently random values vulnerability exists in Vnet/IP communication module VI461 of YOKOGAWA Wide Area Communication Router (WAC Router) AW810D, which may allow a remote attacker to cause denial-of-service (DoS) condition by sending a specially crafted packet.	7.5	More Details
CVE-2022-32084	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component sub_select.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32091	MariaDB v10.7 was discovered to contain an use-after-poison in in __interceptor_memset at /libsanitizer/sanitizer_common/sanitizer_common_interceptors.inc.	7.5	More Details
CVE-2022-23720	PingID Windows Login prior to 2.8 does not alert or halt operation if it has been provisioned with the full permissions PingID properties file. An IT administrator could mistakenly deploy administrator privileged PingID API credentials, such as those typically used by PingFederate, into PingID Windows Login user endpoints. Using sensitive full permissions properties file outside of a privileged trust boundary leads to an increased risk of exposure or discovery, and an attacker could leverage these credentials to perform administrative actions against PingID APIs or endpoints.	7.5	More Details
CVE-2022-32046	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the desc parameter in the function FUN_0041880c.	7.5	More Details
CVE-2022-32047	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the desc parameter in the function FUN_00412ef4.	7.5	More Details
CVE-2014-3648	The simplepush server iterates through the application installations and pushes a notification to the server provided by deviceToken. But this is user controlled. If a bogus applications is registered with bad deviceTokens, one can generate endless exceptions when those endpoints can't be reached or can slow the server down by purposefully wasting it's time with slow endpoints. Similarly, one can provide whatever HTTP end point they want. This turns the server into a DDOS vector or an anonymizer for the posting of malware and so on.	7.5	More Details
CVE-2022-32048	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the command parameter in the function FUN_0041cc88.	7.5	More Details
CVE-2022-33099	An issue in the component luaG_runerror of Lua v5.4.4 and below leads to a heap-buffer overflow when a recursive error occurs.	7.5	More Details
CVE-2022-32049	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the url parameter in the function FUN_00418540.	7.5	More Details
CVE-2022-32050	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the cloneMac parameter in the function FUN_0041af40.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32051	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the desc, week, sTime, eTime parameters in the function FUN_004133c4.	7.5	More Details
CVE-2022-33087	A stack overflow in the function DM_ In fillobjbystr() of TP-Link Archer C50&A5(US)_V5_200407 allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	7.5	More Details
CVE-2022-33082	An issue in the AST parser (ast/compile.go) of Open Policy Agent v0.10.2 allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2022-32043	Tenda M3 V1.0.0.12 was discovered to contain a stack overflow via the function formSetAccessCodeInfo.	7.5	More Details
CVE-2022-32052	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the desc parameter in the function FUN_004137a4.	7.5	More Details
CVE-2022-32053	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the cloneMac parameter in the function FUN_0041621c.	7.5	More Details
CVE-2022-32081	MariaDB v10.4 to v10.7 was discovered to contain an use-after-poison in prepare_inplace_add_virtual at /storage/innobase/handler/handler0alter.cc.	7.5	More Details
CVE-2022-32082	MariaDB v10.5 to v10.7 was discovered to contain an assertion failure at table->get_ref_count() == 0 in dict0dict.cc.	7.5	More Details
CVE-2022-32083	MariaDB v10.2 to v10.6.1 was discovered to contain a segmentation fault via the component Item_subselect::init_expr_cache_tracker.	7.5	More Details
CVE-2022-32085	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component Item_func_in::cleanup/Item::cleanup_processor.	7.5	More Details
CVE-2022-32086	MariaDB v10.4 to v10.8 was discovered to contain a segmentation fault via the component Item_field::fix_outer_field.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32087	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component Item_args::walk_args.	7.5	More Details
CVE-2022-32088	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component Exec_time_tracker::get_loops/Filesort_tracker::report_use/filesort.	7.5	More Details
CVE-2022-32089	MariaDB v10.5 to v10.7 was discovered to contain a segmentation fault via the component st_select_lex_unit::exclude_level.	7.5	More Details
CVE-2022-32044	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the password parameter in the function FUN_00413f80.	7.5	More Details
CVE-2022-32040	Tenda M3 V1.0.0.12 was discovered to contain a stack overflow via the function formSetCfm.	7.5	More Details
CVE-2022-32045	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the desc parameter in the function FUN_00413be4.	7.5	More Details
CVE-2022-33023	CVA6 commit 909d85a gives incorrect permission to use special multiplication units when the format of instructions is wrong.	7.5	More Details
CVE-2022-2306	Old session tokens can be used to authenticate to the application and send authenticated requests.	7.5	More Details
CVE-2022-30290	In OpenCTI through 5.2.4, a broken access control vulnerability has been identified in the profile endpoint. An attacker can abuse the identified vulnerability in order to arbitrarily change their registered e-mail address as well as their API key, even though such action is not possible through the interface, legitimately.	7.5	More Details
CVE-2022-32035	Tenda M3 V1.0.0.12 was discovered to contain a stack overflow via the function formMasterMng.	7.5	More Details
CVE-2022-32034	Tenda M3 V1.0.0.12 was discovered to contain a stack overflow via the items parameter in the function formdelMasteraclist.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31600	NVIDIA DGX A100 contains a vulnerability in SBIOS in the SmmCore, where a user with high privileges can chain another vulnerability to this vulnerability, causing an integer overflow, possibly leading to code execution, escalation of privileges, denial of service, compromised integrity, and information disclosure. The scope of impact can extend to other components.	7.5	More Details
CVE-2022-2229	An improper authorization issue in GitLab CE/EE affecting all versions from 13.7 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows an attacker to extract the value of an unprotected variable they know the name of in public projects or private projects they're a member of.	7.5	More Details
CVE-2022-34829	Zoho ManageEngine ADSelfService Plus before 6203 allows a denial of service (application restart) via a crafted payload to the Mobile App Deployment API.	7.5	More Details
CVE-2022-32036	Tenda M3 V1.0.0.12 was discovered to contain multiple stack overflow vulnerabilities via the ssidList, storeName, and trademark parameters in the function formSetStoreWeb.	7.5	More Details
CVE-2022-2309	NULL Pointer Dereference allows attackers to cause a denial of service (or application crash). This only applies when lxml is used together with libxml2 2.9.10 through 2.9.14. libxml2 2.9.9 and earlier are not affected. It allows triggering crashes through forged input data, given a vulnerable code sequence in the application. The vulnerability is caused by the iterwalk function (also used by the canonicalize function). Such code shouldn't be in wide-spread use, given that parsing + iterwalk would usually be replaced with the more efficient iterparse function. However, an XML converter that serialises to C14N would also be vulnerable, for example, and there are legitimate use cases for this code sequence. If untrusted input is received (also remotely) and processed via iterwalk function, a crash can be triggered.	7.5	More Details
CVE-2022-32037	Tenda M3 V1.0.0.12 was discovered to contain a stack overflow via the function formSetAPCfg.	7.5	More Details
CVE-2022-32031	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow via the list parameter in the function fromSetRouteStatic.	7.5	More Details
CVE-2022-33021	CVA6 commit 909d85a accesses invalid memory when reading the value of MHPMCOUNTER30.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22474	IBM Spectrum Protect 8.1.0.0 through 8.1.14.0 dsmcad, dsmc, and dsmcsvc processes incorrectly handle certain read operations on TCP/IP sockets. This can result in a denial of service for IBM Spectrum Protect client operations. IBM X-Force ID: 225348.	7.5	More Details
CVE-2022-32039	Tenda M3 V1.0.0.12 was discovered to contain a stack overflow via the listN parameter in the function fromDhcpListClient.	7.5	More Details
CVE-2022-32033	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow via the function formSetVirtualSer.	7.5	More Details
CVE-2022-31116	UltraJSON is a fast JSON encoder and decoder written in pure C with bindings for Python 3.7+. Affected versions were found to improperly decode certain characters. JSON strings that contain escaped surrogate characters not part of a proper surrogate pair were decoded incorrectly. Besides corrupting strings, this allowed for potential key confusion and value overwriting in dictionaries. All users parsing JSON from untrusted sources are vulnerable. From version 5.4.0, UltraJSON decodes lone surrogates in the same way as the standard library's `json` module does, preserving them in the parsed output. Users are advised to upgrade. There are no known workarounds for this issue.	7.5	More Details
CVE-2022-34043	Incorrect permissions for the folder C:\ProgramData\NoMachine\var\uninstall of Nomachine v7.9.2 allows attackers to perform a DLL hijacking attack and execute arbitrary code.	7.3	More Details
CVE-2017-20111	A vulnerability, which was classified as critical, was found in Teleopti WFM 7.1.0. This affects an unknown part of the component Administration. The manipulation leads to improper privilege management. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue.	7.3	More Details
CVE-2022-33061	Online Railway Reservation System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Master.php?f=delete_service.	7.2	More Details
CVE-2022-33058	Online Railway Reservation System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Master.php?f=delete_message.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23719	PingID Windows Login prior to 2.8 does not authenticate communication with a local Java service used to capture security key requests. An attacker with the ability to execute code on the target machine maybe able to exploit and spoof the local Java service using multiple attack vectors. A successful attack can lead to code executed as SYSTEM by the PingID Windows Login application, or even a denial of service for offline security key authentication.	7.2	More Details
CVE-2022-32412	An issue in the /template/edit component of HongCMS v3.0 allows attackers to getshell.	7.2	More Details
CVE-2022-33057	Online Railway Reservation System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Master.php?f=delete_reservation.	7.2	More Details
CVE-2022-2073	Code Injection in GitHub repository getgrav/grav prior to 1.7.34.	7.2	More Details
CVE-2022-33060	Online Railway Reservation System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Master.php?f=delete_schedule.	7.2	More Details
CVE-2022-33059	Online Railway Reservation System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Master.php?f=delete_train.	7.2	More Details
CVE-2021-37770	Nucleus CMS v3.71 is affected by a file upload vulnerability. In this vulnerability, we can use upload to change the upload path to the path without the Htaccess file. Upload an Htaccess file and write it to AddType application / x-httpd-php.jpg. In this way, an attacker can upload a picture with shell, treat it as PHP, execute commands, so as to take down website resources.	7.2	More Details
CVE-2022-31058	Tuleap is a Free & Open Source Suite to improve management of software developments and collaboration. In versions prior to 13.9.99.95 Tuleap does not sanitize properly user inputs when constructing the SQL query to retrieve data for the tracker reports. An attacker with the capability to create a new tracker can execute arbitrary SQL queries. Users are advised to upgrade. There is no known workaround for this issue.	7.2	More Details
CVE-2022-33042	Online Railway Reservation System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/inquiries/view_details.php.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2268	The Import any XML or CSV File to WordPress plugin before 3.6.8 accepts all zip files and automatically extracts the zip file without validating the extracted file type. Allowing high privilege users such as admin to upload an arbitrary file like PHP, leading to RCE	7.2	More Details
CVE-2022-33085	ESPCMS P8 was discovered to contain an authenticated remote code execution (RCE) vulnerability via the fetch_filename function at \espcms_public\espcms_templates\ESPCMS_Templates.	7.2	More Details
CVE-2021-44915	Taocms 3.0.2 was discovered to contain a blind SQL injection vulnerability via the function Edit category.	7.2	More Details
CVE-2022-32411	An issue in the languages config file of HongCMS v3.0 allows attackers to getshell.	7.2	More Details
CVE-2022-26365	Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Linux Block and Network PV device frontends don't zero memory regions before sharing them with the backend (CVE-2022-26365, CVE-2022-33740). Additionally the granularity of the grant table doesn't allow sharing less than a 4K page, leading to unrelated data residing in the same 4K page as data shared with a backend being accessible by such backend (CVE-2022-33741, CVE-2022-33742).	7.1	More Details
CVE-2022-2287	Out-of-bounds Read in GitHub repository vim/vim prior to 9.0.	7.1	More Details
CVE-2022-33740	Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Linux Block and Network PV device frontends don't zero memory regions before sharing them with the backend (CVE-2022-26365, CVE-2022-33740). Additionally the granularity of the grant table doesn't allow sharing less than a 4K page, leading to unrelated data residing in the same 4K page as data shared with a backend being accessible by such backend (CVE-2022-33741, CVE-2022-33742).	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33741	Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Linux Block and Network PV device frontends don't zero memory regions before sharing them with the backend (CVE-2022-26365, CVE-2022-33740). Additionally the granularity of the grant table doesn't allow sharing less than a 4K page, leading to unrelated data residing in the same 4K page as data shared with a backend being accessible by such backend (CVE-2022-33741, CVE-2022-33742).	7.1	More Details
CVE-2022-33742	Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Linux Block and Network PV device frontends don't zero memory regions before sharing them with the backend (CVE-2022-26365, CVE-2022-33740). Additionally the granularity of the grant table doesn't allow sharing less than a 4K page, leading to unrelated data residing in the same 4K page as data shared with a backend being accessible by such backend (CVE-2022-33741, CVE-2022-33742).	7.1	More Details
CVE-2022-27904	Automox Agent for macOS before version 39 was vulnerable to a time-of-check/time-of-use (TOCTOU) race-condition attack during the agent install process.	7.0	More Details
CVE-2022-30467	Joy ebike Wolf Manufacturing year 2022 is vulnerable to Denial of service, which allows remote attackers to jam the key fob request via RF.	6.8	More Details
CVE-2022-31601	NVIDIA DGX A100 contains a vulnerability in SBIOS in the SmbiosPei, which may allow a highly privileged local attacker to cause an out-of-bounds write, which may lead to code execution, denial of service, compromised integrity, and information disclosure.	6.7	More Details
CVE-2022-32325	JPEGOPTIM v1.4.7 was discovered to contain a segmentation violation which is caused by a READ memory access at jpegoptim.c.	6.5	More Details
CVE-2022-34794	Missing permission checks in Jenkins Recipe Plugin 1.2 and earlier allow attackers with Overall/Read permission to send an HTTP request to an attacker-specified URL and parse the response as XML.	6.5	More Details
CVE-2022-29271	In Nagios XI through 5.8.5, a read-only Nagios user (due to an incorrect permission check) is able to schedule downtime for any host/services. This allows an attacker to permanently disable all monitoring checks.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1983	Incorrect authorization in GitLab EE affecting all versions from 10.7 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allowed an attacker already in possession of a valid Deploy Key or a Deploy Token to misuse it from any location to access Container Registries even when IP address restrictions were configured.	6.5	More Details
CVE-2022-1967	The WP Championship WordPress plugin before 9.3 is lacking CSRF checks in various places, allowing attackers to make a logged in admin perform unwanted actions, such as create and delete arbitrary teams as well as update the plugin's settings. Due to the lack of sanitisation and escaping, it could also lead to Stored Cross-Site Scripting issues	6.5	More Details
CVE-2022-34879	Reflected Cross Site Scripting (XSS) vulnerabilities in AST Agent Time Sheet interface (/vicidial/AST_agent_time_sheet.php) of VICIdial via agent, and search_archived_data parameters. This issue affects: VICIdial 2.14b0.5 versions prior to 3555.	6.5	More Details
CVE-2022-34780	A cross-site request forgery (CSRF) vulnerability in Jenkins XebiaLabs XL Release Plugin 22.0.0 and earlier allows attackers to connect to an attacker-specified HTTP server using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	6.5	More Details
CVE-2022-34781	Missing permission checks in Jenkins XebiaLabs XL Release Plugin 22.0.0 and earlier allow attackers with Overall/Read permission to connect to an attacker-specified HTTP server using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	6.5	More Details
CVE-2022-29892	Improper input validation vulnerability in Space of Cybozu Garoon 4.0.0 to 5.5.1 allows a remote authenticated attacker to repeatedly display errors in certain functions and cause a denial-of-service (DoS).	6.5	More Details
CVE-2022-29269	In Nagios XI through 5.8.5, in the schedule report function, an authenticated attacker is able to inject HTML tags that lead to the reformatting/editing of emails from an official email address.	6.5	More Details
CVE-2022-34789	A cross-site request forgery (CSRF) vulnerability in Jenkins Matrix Reloaded Plugin 1.1.3 and earlier allows attackers to rebuild previous matrix builds.	6.5	More Details
CVE-2022-34816	Jenkins HPE Network Virtualization Plugin 1.0 stores passwords unencrypted in its global configuration file on the Jenkins controller where they can be viewed by users with access to the Jenkins controller file system.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22496	While a user account for the IBM Spectrum Protect Server 8.1.0.000 through 8.1.14 is being established, it may be configured to use SESSIONSECURITY=TRANSITIONAL. While in this mode, it may be susceptible to an offline dictionary attack. IBM X-Force ID: 226942.	6.5	More Details
CVE-2022-34805	Jenkins Skype notifier Plugin 1.1.0 and earlier stores a password unencrypted in its global configuration file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.	6.5	More Details
CVE-2022-34903	GnuPG through 2.3.6, in unusual situations where an attacker possesses any secret-key information from a victim's keyring and other constraints (e.g., use of GPGME) are met, allows signature forgery via injection into the status line.	6.5	More Details
CVE-2022-31063	Tuleap is a Free & Open Source Suite to improve management of software developments and collaboration. In versions prior to 13.9.99.111 the title of a document is not properly escaped in the search result of MyDocmanSearch widget and in the administration page of the locked documents. A malicious user with the capability to create a document could force victim to execute uncontrolled code. Users are advised to upgrade. There are no known workarounds for this issue.	6.5	More Details
CVE-2022-34810	A missing check in Jenkins RQM Plugin 2.8 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	6.5	More Details
CVE-2022-34809	Jenkins RQM Plugin 2.8 and earlier stores a password unencrypted in its global configuration file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.	6.5	More Details
CVE-2022-26135	A vulnerability in Mobile Plugin for Jira Data Center and Server allows a remote, authenticated user (including a user who joined via the sign-up feature) to perform a full read server-side request forgery via a batch endpoint. This affects Atlassian Jira Server and Data Center from version 8.0.0 before version 8.13.22, from version 8.14.0 before 8.20.10, from version 8.21.0 before 8.22.4. This also affects Jira Management Server and Data Center versions from version 4.0.0 before 4.13.22, from version 4.14.0 before 4.20.10 and from version 4.21.0 before 4.22.4.	6.5	More Details
CVE-2022-34807	Jenkins Elasticsearch Query Plugin 1.2 and earlier stores a password unencrypted in its global configuration file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34806	Jenkins Jigomerge Plugin 0.9 and earlier stores passwords unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Extended Read permission, or access to the Jenkins controller file system.	6.5	More Details
CVE-2022-34877	SQL Injection vulnerability in AST Agent Time Sheet interface ((/vicidial/AST_agent_time_sheet.php) of VICIdial via the agent parameter allows attacker to spoof identity, tamper with existing data, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server. This issue affects: VICIdial 2.14b0.5 versions prior to 3555.	6.4	More Details
CVE-2022-31603	NVIDIA DGX A100 contains a vulnerability in SBIOS in the IpSecDxe, where a user with high privileges and preconditioned IpSecDxe global data can exploit improper validation of an array index to cause code execution, which may lead to denial of service, data integrity impact, and information disclosure.	6.4	More Details
CVE-2022-31602	NVIDIA DGX A100 contains a vulnerability in SBIOS in the IpSecDxe, where a user with elevated privileges and a preconditioned heap can exploit an out-of-bounds write vulnerability, which may lead to code execution, denial of service, data integrity impact, and information disclosure.	6.4	More Details
CVE-2022-31113	Canarytokens is an open source tool which helps track activity and actions on your network. A Cross-Site Scripting vulnerability was identified in the history page of triggered Canarytokens. This permits an attacker who recognised an HTTP-based Canarytoken (a URL) to execute Javascript in the Canarytoken's history page (domain: canarytokens.org) when the history page is later visited by the Canarytoken's creator. This vulnerability could be used to disable or delete the affected Canarytoken, or view its activation history. It might also be used as a stepping stone towards revealing more information about the Canarytoken's creator to the attacker. For example, an attacker could recover the email address tied to the Canarytoken, or place Javascript on the history page that redirect the creator towards an attacker-controlled Canarytoken to show the creator's network location. An attacker could only act on the discovered Canarytoken. This issue did not expose other Canarytokens or other Canarytoken creators. The issue has been patched on Canarytokens.org and in the latest release. No signs of successful exploitation of this vulnerability have been found. Users are advised to upgrade. There are no known workarounds for this issue.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-20124	A vulnerability classified as critical has been found in Online Hotel Booking System Pro Plugin 1.0. Affected is an unknown function of the file /front/roomtype-details.php. The manipulation of the argument tid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2017-20125	A vulnerability classified as critical was found in Online Hotel Booking System Pro 1.2. Affected by this vulnerability is an unknown functionality of the file /roomtype-details.php. The manipulation of the argument tid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2022-2254	A user with administrative privileges in Distributed Data Systems WebHMI 4.1.1.7662 can store a script that could impact other logged in users.	6.2	More Details
CVE-2022-25876	The package link-preview-js before 2.1.16 are vulnerable to Server-side Request Forgery (SSRF) which allows attackers to send arbitrary requests to the local network and read the response. This is due to flawed DNS rebinding protection.	6.2	More Details
CVE-2022-34912	An issue was discovered in MediaWiki before 1.37.3 and 1.38.x before 1.38.1. The contributions-title, used on Special:Contributions, is used as page title without escaping. Hence, in a non-default configuration where a username contains HTML entities, it won't be escaped.	6.1	More Details
CVE-2022-27627	Cross-site scripting vulnerability in Organization's Information of Cybozu Garoon 4.10.2 to 5.5.1 allows a remote attacker to execute an arbitrary script on the logged-in user's web browser.	6.1	More Details
CVE-2021-37524	Cross Site Scripting (XSS) vulnerability in FusionPBX 4.5.26 allows remote unauthenticated users to inject arbitrary web script or HTML via an unsanitized "path" parameter in resources/login.php.	6.1	More Details
CVE-2020-26877	ApiFest OAuth 2.0 Server 0.3.1 does not validate the redirect URI in accordance with RFC 6749 and is susceptible to an open redirector attack. Specifically, it directly sends an authorization code to the redirect URI submitted with the authorization request, without checking whether the redirect URI is registered by the client who initiated the request. This allows an attacker to craft a request with a manipulated redirect URI (redirect_uri parameter), which is under the attacker's control, and consequently obtain the leaked authorization code when the server redirects the client to the manipulated redirect URI with an authorization code. NOTE: this is similar to CVE-2019-3778.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39074	IBM Security Guardium 11.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	6.1	More Details
CVE-2022-2252	Open Redirect in GitHub repository microweber/microweber prior to 1.2.19.	6.1	More Details
CVE-2022-0250	The Redirection for Contact Form 7 WordPress plugin before 2.5.0 does not escape a link generated before outputting it in an attribute, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-1946	The Gallery WordPress plugin before 2.0.0 does not sanitise and escape a parameter before outputting it back in the response of an AJAX action (available to both unauthenticated and authenticated users), leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2022-31897	SourceCodester Zoo Management System 1.0 is vulnerable to Cross Site Scripting (XSS) via public_html/register_visitor?msg=.	6.1	More Details
CVE-2013-4170	In general, Ember.js escapes or strips any user-supplied content before inserting it in strings that will be sent to innerHTML. However, the `tagName` property of an `Ember.View` was inserted into such a string without being sanitized. This means that if an application assigns a view's `tagName` to user-supplied data, a specially-crafted payload could execute arbitrary JavaScript in the context of the current domain ("XSS"). This vulnerability only affects applications that assign or bind user-provided content to `tagName`.	6.1	More Details
CVE-2022-29272	In Nagios XI through 5.8.5, an open redirect vulnerability exists in the login function that could lead to spoofing.	6.1	More Details
CVE-2022-2290	Cross-site Scripting (XSS) - Reflected in GitHub repository zadam/trilium prior to 0.52.4, 0.53.1-beta.	6.1	More Details
CVE-2022-34911	An issue was discovered in MediaWiki before 1.35.7, 1.36.x and 1.37.x before 1.37.3, and 1.38.x before 1.38.1. XSS can occur in configurations that allow a JavaScript payload in a username. After account creation, when it sets the page title to "Welcome" followed by the username, the username is not escaped: SpecialCreateAccount::successfulAction() calls ::showSuccessPage() with a message as second parameter, and OutputPage::setPageTitle() uses text().	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32969	MetaMask before 10.11.3 might allow an attacker to access a user's secret recovery phrase because an input field is used for a BIP39 mnemonic, and Firefox and Chromium save such fields to disk in order to support the Restore Session feature, aka the Demonic issue.	5.9	More Details
CVE-2022-31117	UltraJSON is a fast JSON encoder and decoder written in pure C with bindings for Python 3.7+. In versions prior to 5.4.0 an error occurring while reallocating a buffer for string decoding can cause the buffer to get freed twice. Due to how UltraJSON uses the internal decoder, this double free is impossible to trigger from Python. This issue has been resolved in version 5.4.0 and all users should upgrade to UltraJSON 5.4.0. There are no known workarounds for this issue.	5.9	More Details
CVE-2022-2279	NULL Pointer Dereference in GitHub repository bfabiszewski/libmobi prior to 0.11.	5.5	More Details
CVE-2014-0068	It was reported that watchman in openshift node-utils creates /var/run/watchman.pid and /var/log/watchman.ouput with world writable permission.	5.5	More Details
CVE-2022-2301	Buffer Over-read in GitHub repository hpjansson/chafa prior to 1.10.3.	5.5	More Details
CVE-2022-22478	IBM Spectrum Protect Client 8.1.0.0 through 8.1.14.0 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 225886.	5.5	More Details
CVE-2022-2058	Divide By Zero error in tiffcrop in libtiff 4.4.0 allows attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit f3a5e010.	5.5	More Details
CVE-2022-2057	Divide By Zero error in tiffcrop in libtiff 4.4.0 allows attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit f3a5e010.	5.5	More Details
CVE-2022-2056	Divide By Zero error in tiffcrop in libtiff 4.4.0 allows attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit f3a5e010.	5.5	More Details
CVE-2022-2078	A vulnerability was found in the Linux kernel's nft_set_desc_concat_parse() function .This flaw allows an attacker to trigger a buffer overflow via nft_set_desc_concat_parse() , causing a denial of service and possibly to run code.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1852	A NULL pointer dereference flaw was found in the Linux kernel's KVM module, which can lead to a denial of service in the x86_emulate_insn in arch/x86/kvm/emulate.c. This flaw occurs while executing an illegal instruction in guest in the Intel CPU.	5.5	More Details
CVE-2022-34876	SQL Injection vulnerability in admin interface (/vicidial/admin.php) of VICIdial via modify_email_accounts, access_recordings, and agentcall_email parameters allows attacker to spoof identity, tamper with existing data, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server. This issue affects: VICIdial 2.14b0.5 versions prior to 3555.	5.5	More Details
CVE-2022-34878	SQL Injection vulnerability in User Stats interface (/vicidial/user_stats.php) of VICIdial via the file_download parameter allows attacker to spoof identity, tamper with existing data, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.	5.5	More Details
CVE-2022-22367	IBM UrbanCode Deploy (UCD) 6.2.7.15, 7.0.5.10, 7.1.2.6, and 7.2.2.1 could disclose sensitive database information to a local user in plain text. IBM X-Force ID: 221008.	5.5	More Details
CVE-2022-26368	Browse restriction bypass and operation restriction bypass vulnerability in Cabinet of Cybozu Garoon 4.0.0 to 5.5.1 allows a remote authenticated attacker to alter and/or obtain the data of Cabinet.	5.4	More Details
CVE-2022-2300	Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 1.2.19.	5.4	More Details
CVE-2022-30289	A stored Cross-site Scripting (XSS) vulnerability was identified in the Data Import functionality of OpenCTI through 5.2.4. An attacker can abuse the vulnerability to upload a malicious file that will then be executed by a victim when they open the file location.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31014	Nextcloud server is an open source personal cloud server. Affected versions were found to be vulnerable to SMTP command injection. The impact varies based on which commands are supported by the backend SMTP server. However, the main risk here is that the attacker can then hijack an already-authenticated SMTP session and run arbitrary SMTP commands as the email user, such as sending emails to other users, changing the FROM user, and so on. As before, this depends on the configuration of the server itself, but newlines should be sanitized to mitigate such arbitrary SMTP command injection. It is recommended that the Nextcloud Server is upgraded to 22.2.8 , 23.0.5 or 24.0.1. There are no known workarounds for this issue.	5.4	More Details
CVE-2022-28803	In SilverStripe Framework through 2022-04-07, Stored XSS can occur in javascript link tags added via XMLHttpRequest (XHR).	5.4	More Details
CVE-2022-22373	An improper validation vulnerability in IBM InfoSphere Information Server 11.7 Pack for SAP Apps and BW Packs may lead to creation of directories and files on the server file system that may contain non-sensitive debugging information like stack traces. IBM X-Force ID: 221323.	5.4	More Details
CVE-2014-3650	Multiple persistent cross-site scripting (XSS) flaws were found in the way Aerogear handled certain user-supplied content. A remote attacker could use these flaws to compromise the application with specially crafted input.	5.4	More Details
CVE-2022-33043	A cross-site scripting (XSS) vulnerability in the batch add function of Urtracker Premium v4.0.1.1477 allows attackers to execute arbitrary web scripts or HTML via a crafted excel file.	5.4	More Details
CVE-2022-34777	Jenkins GitLab Plugin 1.5.34 and earlier does not escape multiple fields inserted into the description of webhook-triggered builds, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-34778	Jenkins TestNG Results Plugin 554.va4a552116332 and earlier renders the unescaped test descriptions and exception messages provided in test results if certain job-level options are set, resulting in a cross-site scripting (XSS) vulnerability exploitable by attackers able to configure jobs or control test results.	5.4	More Details
CVE-2022-34783	Jenkins Plot Plugin 2.1.10 and earlier does not escape plot descriptions, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34784	Jenkins build-metrics Plugin 1.3 does not escape the build description on one of its views, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Build/Update permission.	5.4	More Details
CVE-2022-34786	Jenkins Rich Text Publisher Plugin 1.4 and earlier does not escape the HTML message set by its post-build step, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to configure jobs.	5.4	More Details
CVE-2022-34787	Jenkins Project Inheritance Plugin 21.04.03 and earlier does not escape the reason a build is blocked in tooltips, resulting in a cross-site scripting (XSS) vulnerability exploitable by attackers able to control the reason a queue item is blocked.	5.4	More Details
CVE-2022-34788	Jenkins Matrix Reloaded Plugin 1.1.3 and earlier does not escape the agent name in tooltips, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Agent/Configure permission.	5.4	More Details
CVE-2022-34790	Jenkins eXtreme Feedback Panel Plugin 2.0.1 and earlier does not escape the job names used in tooltips, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-34791	Jenkins Validating Email Parameter Plugin 1.10 and earlier does not escape the name and description of its parameter type, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
	Cross Site Scripting (XSS) vulnerability in router Asus DSL-N14U-B1 1.1.2.3_805 via the "*list" parameters (e.g. filter_lwlist, keyword_rulelist, etc) in every ".asp" page containing a list of stored strings. The following asp files are affected: (1) cgi-bin/APP_Installation.asp, (2) cgi-bin/Advanced_ACL_Content.asp, (3) cgi-bin/Advanced_ADSL_Content.asp, (4) cgi-bin/Advanced_ASUSDDNS_Content.asp, (5) cgi-bin/Advanced_AiDisk_ftp.asp, (6) cgi-bin/Advanced_AiDisk_samba.asp, (7) cgi-bin/Advanced_DSL_Content.asp, (8) cgi-bin/Advanced_Firewall_Content.asp, (9) cgi-bin/Advanced_FirmwareUpgrade_Content.asp, (10) cgi-bin/Advanced_GWStaticRoute_Content.asp, (11) cgi-bin/Advanced_IPTV_Content.asp, (12) cgi-bin/Advanced_IPv6_Content.asp, (13) cgi-bin/Advanced_KeywordFilter_Content.asp, (14) cgi-bin/Advanced_LAN_Content.asp, (15) cgi-bin/Advanced_Modem_Content.asp, (16) cgi-bin/Advanced_PortTrigger_Content.asp, (17) cgi-		

CVE Number	Description	Base Score	Reference
	bin/Advanced_QOSUserPrio_Content.asp, (18) cgi-bin/Advanced_QOSUserRules_Content.asp, (19) cgi-bin/Advanced_SettingBackup_Content.asp, (20) cgi-		
CVE-2022-32988	bin/Advanced_System_Content.asp, (21) cgi-bin/Advanced_URLFilter_Content.asp, (22) cgi-bin/Advanced_VPN_PPTP.asp, (23) cgi-bin/Advanced_VirtualServer_Content.asp, (24) cgi-bin/Advanced_WANPort_Content.asp, (25) cgi-bin/Advanced_WAdvanced_Content.asp, (26) cgi-bin/Advanced_WMode_Content.asp, (27) cgi-bin/Advanced_WWPS_Content.asp, (28) cgi-bin/Advanced_Wireless_Content.asp, (29) cgi-bin/Bandwidth_Limiter.asp, (30) cgi-bin/Guest_network.asp, (31) cgi-bin/Main_AccessLog_Content.asp, (32) cgi-bin/Main_AdslStatus_Content.asp, (33) cgi-bin/Main_Spectrum_Content.asp, (34) cgi-bin/Main_WebHistory_Content.asp, (35) cgi-bin/ParentalControl.asp, (36) cgi-bin/QIS_wizard.asp, (37) cgi-bin/QoS_EZQoS.asp, (38) cgi-bin/aidisk.asp, (39) cgi-bin/aidisk/Aidisk-1.asp, (40) cgi-bin/aidisk/Aidisk-2.asp, (41) cgi-bin/aidisk/Aidisk-3.asp, (42) cgi-bin/aidisk/Aidisk-4.asp, (43) cgi-bin/blocking.asp, (44) cgi-bin/cloud_main.asp, (45) cgi-bin/cloud_router_sync.asp, (46) cgi-bin/cloud_settings.asp, (47) cgi-bin/cloud_sync.asp, (48) cgi-bin/device-map/DSL_dashboard.asp, (49) cgi-bin/device-map/clients.asp, (50) cgi-bin/device-map/disk.asp, (51) cgi-bin/device-map/internet.asp, (52) cgi-bin/error_page.asp, (53) cgi-bin/index.asp, (54) cgi-bin/index2.asp, (55) cgi-bin/qis/QIS_PTM_manual_setting.asp, (56) cgi-bin/qis/QIS_admin_pass.asp, (57) cgi-bin/qis/QIS_annex_setting.asp, (58) cgi-bin/qis/QIS_bridge_cfg_tmp.asp, (59) cgi-bin/qis/QIS_detect.asp, (60) cgi-bin/qis/QIS_finish.asp, (61) cgi-bin/qis/QIS_ipoa_cfg_tmp.asp, (62) cgi-bin/qis/QIS_manual_setting.asp, (63) cgi-bin/qis/QIS_mer_cfg.asp, (64) cgi-bin/qis/QIS_mer_cfg_tmp.asp, (65) cgi-bin/qis/QIS_ppp_cfg.asp, (66) cgi-bin/qis/QIS_ppp_cfg_tmp.asp, (67) cgi-bin/qis/QIS_wireless.asp, (68) cgi-bin/query_wan_status.asp, (69) cgi-bin/query_wan_status2.asp, and (70) cgi-bin/start_apply.asp.	5.4	More Details
CVE-2022-2280	Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 1.2.19.	5.4	More Details
CVE-2022-34795	Jenkins Deployment Dashboard Plugin 1.0.10 and earlier does not escape environment names on its Deployment Dashboard view, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with View/Configure permission.	5.4	More Details
CVE-2022-33075	A stored cross-site scripting (XSS) vulnerability in the Add Classification function of Zoo Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via unspecified vectors.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31110	RSSHub is an open source, extensible RSS feed generator. In commits prior to 5c4177441417 passing some special values to the `filter` and `filterout` parameters can cause an abnormally high CPU. This results in an impact on the performance of the servers and RSSHub services which may lead to a denial of service. This issue has been fixed in commit 5c4177441417 and all users are advised to upgrade. There are no known workarounds for this issue.	5.3	More Details
CVE-2022-1963	An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.4 before 14.10.5, all versions starting from 15.0 before 15.0.4, all versions starting from 15.1 before 15.1.1. GitLab reveals if a user has enabled two-factor authentication on their account in the HTML source, to unauthenticated users.	5.3	More Details
CVE-2022-28713	Improper authentication vulnerability in Scheduler of Cybozu Garoon 4.10.0 to 5.5.1 allows a remote attacker to obtain some data of Facility Information without logging in to the product.	5.3	More Details
CVE-2022-2228	Information exposure in GitLab EE affecting all versions from 12.0 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows an attacker with the appropriate access tokens to obtain CI variables in a group with using IP-based access restrictions even if the GitLab Runner is calling from outside the allowed IP range	5.3	More Details
CVE-2022-2097	AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of "in place" encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p).	5.3	More Details
CVE-2022-22494	IBM Spectrum Protect Operations Center 8.1.0.000 through 8.1.14 could allow a remote attacker to gain details of the database, such as type and version, by sending a specially-crafted HTTP request. This information could then be used in future attacks. IBM X-Force ID: 226940.	5.3	More Details
CVE-2022-25758	All versions of package scss-tokenizer are vulnerable to Regular Expression Denial of Service (ReDoS) via the loadAnnotation() function, due to the usage of insecure regex.	5.3	More Details
CVE-2022-23717	PingID Windows Login prior to 2.8 is vulnerable to a denial of service condition on local machines when combined with using offline security keys as part of authentication.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2243	An access control vulnerability in GitLab EE/CE affecting all versions from 14.8 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows authenticated users to enumerate issues in non-linked sentry projects.	5.0	More Details
CVE-2022-31770	IBM App Connect Enterprise Certified Container 4.2 could allow a user from the administration console to cause a denial of service by creating a specially crafted request. IBM X-Force ID: 228221.	4.9	More Details
CVE-2021-37791	MyAdmin v1.0 is affected by an incorrect access control vulnerability in viewing personal center in /api/user/userData?userCode=admin.	4.9	More Details
CVE-2021-25066	The Ninja Forms Contact Form WordPress plugin before 3.6.10 does not sanitize and escape some imported data, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2022-29513	Cross-site scripting vulnerability in Scheduler of Cybozu Garoon 4.10.0 to 5.5.1 allows a remote authenticated attacker with an administrative privilege to execute an arbitrary script.	4.8	More Details
CVE-2021-25056	The Ninja Forms Contact Form WordPress plugin before 3.6.10 does not sanitise and escape field labels, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2022-25896	This affects the package passport before 0.6.0. When a user logs in or logs out, the session is regenerated instead of being closed.	4.8	More Details
CVE-2022-1301	The WP Contact Slider WordPress plugin before 2.4.7 does not sanitize and escape the Text to Display settings of sliders, which could allow high privileged users such as editor and above to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed	4.8	More Details
CVE-2022-2250	An open redirect vulnerability in GitLab EE/CE affecting all versions from 11.1 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows an attacker to redirect users to an arbitrary location if they trust the URL.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33744	Arm guests can cause Dom0 DoS via PV devices When mapping pages of guests on Arm, dom0 is using an rbtree to keep track of the foreign mappings. Updating of that rbtree is not always done completely with the related lock held, resulting in a small race window, which can be used by unprivileged guests via PV devices to cause inconsistencies of the rbtree. These inconsistencies can lead to Denial of Service (DoS) of dom0, e.g. by causing crashes or the inability to perform further mappings of other guests' memory pages.	4.7	More Details
CVE-2022-1955	Session 1.13.0 allows an attacker with physical access to the victim's device to bypass the application's password/pin lock to access user data. This is possible due to lack of adequate security controls to prevent dynamic code manipulation.	4.6	More Details
CVE-2022-22366	IBM UrbanCode Deploy (UCD) 6.2.7.15, 7.0.5.10, 7.1.2.6, and 7.2.2.1 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 22106.	4.4	More Details
CVE-2022-27807	Improper input validation vulnerability in Link of Cybozu Garoon 4.0.0 to 5.5.1 allows a remote authenticated attacker to disable to add Categories.	4.3	More Details
CVE-2022-29471	Browse restriction bypass vulnerability in Bulletin of Cybozu Garoon allows a remote authenticated attacker to obtain the data of Bulletin.	4.3	More Details
CVE-2022-28692	Improper input validation vulnerability in Scheduler of Cybozu Garoon 4.0.0 to 5.5.1 allows a remote authenticated attacker to alter the data of Scheduler.	4.3	More Details
CVE-2022-27803	Improper input validation vulnerability in Space of Cybozu Garoon 4.0.0 to 5.5.1 allows a remote authenticated attacker to alter the data of Space.	4.3	More Details
CVE-2022-29270	In Nagios XI through 5.8.5, it is possible for a user without password verification to change his e-mail address.	4.3	More Details
CVE-2022-26054	Operation restriction bypass vulnerability in Link of Cybozu Garoon 4.0.0 to 5.5.1 allows a remote authenticated attacker to alter the data of Link.	4.3	More Details
CVE-2022-28718	Operation restriction bypass vulnerability in Bulletin of Cybozu Garoon 4.0.0 to 5.5.1 allow a remote authenticated attacker to alter the data of Bulletin.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26051	Operation restriction bypass vulnerability in Portal of Cybozu Garoon 4.0.0 to 5.5.1 allows a remote authenticated attacker to alter the data of Portal.	4.3	More Details
CVE-2022-29467	Address information disclosure vulnerability in Cybozu Garoon 4.2.0 to 5.5.1 allows a remote authenticated attacker to obtain some data of Address.	4.3	More Details
CVE-2017-20110	A vulnerability, which was classified as problematic, has been found in Teleopti WFM up to 7.1.0. Affected by this issue is some unknown functionality of the component Administration. The manipulation as part of JSON leads to information disclosure (Credentials). The attack may be launched remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue.	4.3	More Details
CVE-2022-34785	Jenkins build-metrics Plugin 1.3 and earlier does not perform permission checks in multiple HTTP endpoints, allowing attackers with Overall/Read permission to obtain information about jobs otherwise inaccessible to them.	4.3	More Details
CVE-2022-31266	In ILIAS through 7.10, lack of verification when changing an email address (on the Profile Page) allows remote attackers to take over accounts.	4.3	More Details
CVE-2022-34782	An incorrect permission check in Jenkins requests-plugin Plugin 2.2.16 and earlier allows attackers with Overall/Read permission to view the list of pending requests.	4.3	More Details
CVE-2022-34779	A missing permission check in Jenkins XebiaLabs XL Release Plugin 22.0.0 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details
CVE-2021-38954	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.5 and 6.1.0.0 through 6.1.1.0 could disclose sensitive version information that could aid in future attacks against the system. IBM X-Force ID: 211414.	4.3	More Details
CVE-2022-1954	A Regular Expression Denial of Service vulnerability in GitLab CE/EE affecting all versions from 1.0.2 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows an attacker to make a GitLab instance inaccessible via specially crafted web server response headers	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-20109	A vulnerability classified as problematic was found in Teleopti WFM up to 7.1.0. Affected by this vulnerability is an unknown functionality of the file /TeleoptiWFM/Administration/GetOneTenant of the component Administration. The manipulation leads to information disclosure (Credentials). The attack can be launched remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue.	4.3	More Details
CVE-2022-31032	Tuleap is a Free & Open Source Suite to improve management of software developments and collaboration. In versions prior to 13.9.99.58 authorizations are not properly verified when creating projects or trackers from projects marked as templates. Users can get access to information in those template projects because the permissions model is not properly enforced. Users are advised to upgrade. There are no known workarounds for this issue.	4.3	More Details
CVE-2017-20120	A vulnerability classified as problematic was found in TrueConf Server 4.3.7. This vulnerability affects unknown code of the file /admin/service/stop/. The manipulation leads to cross-site request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2021-40642	Textpattern CMS v4.8.7 and older vulnerability exists through Sensitive Cookie in HTTPS Session Without 'Secure' Attribute via textpattern/lib/txplib_misc.php. The secure flag is not set for txp_login session cookie in the application. If the secure flag is not set, then the cookie will be transmitted in clear-text if the user visits any HTTP URLs within the cookie's scope. An attacker may be able to induce this event by feeding a user suitable links, either directly or via another web site.	4.3	More Details
CVE-2022-2244	An improper authorization vulnerability in GitLab EE/CE affecting all versions from 14.8 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows project memebers with reporter role to manage issues in project's error tracking feature.	4.3	More Details
CVE-2022-27661	Operation restriction bypass vulnerability in Workflow of Cybozu Garoon 4.0.0 to 5.5.1 allows a remote authenticated attacker to alter the data of Workflow.	4.3	More Details
CVE-2022-34796	A missing permission check in Jenkins Deployment Dashboard Plugin 1.0.10 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34804	Jenkins OpsGenie Plugin 1.9 and earlier transmits API keys in plain text as part of the global Jenkins configuration form and job configuration forms, potentially resulting in their exposure.	4.3	More Details
CVE-2022-34797	A cross-site request forgery (CSRF) vulnerability in Jenkins Deployment Dashboard Plugin 1.0.10 and earlier allows attackers to connect to an attacker-specified HTTP URL using attacker-specified credentials.	4.3	More Details
CVE-2022-34818	Jenkins Failed Job Deactivator Plugin 1.2.1 and earlier does not perform permission checks in several views and HTTP endpoints, allowing attackers with Overall/Read permission to disable jobs.	4.3	More Details
CVE-2022-34817	A cross-site request forgery (CSRF) vulnerability in Jenkins Failed Job Deactivator Plugin 1.2.1 and earlier allows attackers to disable jobs.	4.3	More Details
CVE-2022-34815	A cross-site request forgery (CSRF) vulnerability in Jenkins Request Rename Or Delete Plugin 1.1.0 and earlier allows attackers to accept pending requests, thereby renaming or deleting jobs.	4.3	More Details
CVE-2022-34813	A missing permission check in Jenkins XPath Configuration Viewer Plugin 1.1.1 and earlier allows attackers with Overall/Read permission to create and delete XPath expressions.	4.3	More Details
CVE-2022-34812	A cross-site request forgery (CSRF) vulnerability in Jenkins XPath Configuration Viewer Plugin 1.1.1 and earlier allows attackers to create and delete XPath expressions.	4.3	More Details
CVE-2022-34811	A missing permission check in Jenkins XPath Configuration Viewer Plugin 1.1.1 and earlier allows attackers with Overall/Read permission to access the XPath Configuration Viewer page.	4.3	More Details
CVE-2022-34808	Jenkins Cisco Spark Plugin 1.1.1 and earlier stores bearer tokens unencrypted in its global configuration file on the Jenkins controller where they can be viewed by users with access to the Jenkins controller file system.	4.3	More Details
CVE-2022-34814	Jenkins Request Rename Or Delete Plugin 1.1.0 and earlier does not correctly perform a permission check in an HTTP endpoint, allowing attackers with Overall/Read permission to view an administrative configuration page listing pending requests.	4.3	More Details
CVE-2022-34803	Jenkins OpsGenie Plugin 1.9 and earlier stores API keys unencrypted in its global configuration file and in job config.xml files on the Jenkins controller where they can be viewed by users with Extended Read permission (config.xml), or access to the Jenkins controller file system.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34802	Jenkins RocketChat Notifier Plugin 1.5.2 and earlier stores the login password and webhook token unencrypted in its global configuration file on the Jenkins controller where they can be viewed by users with access to the Jenkins controller file system.	4.3	More Details
CVE-2022-34801	Jenkins Build Notifications Plugin 1.5.0 and earlier transmits tokens in plain text as part of the global Jenkins configuration form, potentially resulting in their exposure.	4.3	More Details
CVE-2022-34800	Jenkins Build Notifications Plugin 1.5.0 and earlier stores tokens unencrypted in its global configuration files on the Jenkins controller where they can be viewed by users with access to the Jenkins controller file system.	4.3	More Details
CVE-2022-34799	Jenkins Deployment Dashboard Plugin 1.0.10 and earlier stores a password unencrypted in its global configuration file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.	4.3	More Details
CVE-2022-34798	Jenkins Deployment Dashboard Plugin 1.0.10 and earlier does not perform a permission check in several HTTP endpoints, allowing attackers with Overall/Read permission to connect to an attacker-specified HTTP URL using attacker-specified credentials.	4.3	More Details
CVE-2017-20118	A vulnerability was found in TrueConf Server 4.3.7. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/conferences/list/. The manipulation of the argument domxss leads to basic cross site scripting (DOM). The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2017-20117	A vulnerability was found in TrueConf Server 4.3.7. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/group. The manipulation leads to basic cross site scripting (DOM). The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2017-20116	A vulnerability was found in TrueConf Server 4.3.7. It has been classified as problematic. Affected is an unknown function of the file /admin/group/list/. The manipulation of the argument checked_group_id leads to basic cross site scripting (Reflected). It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-20115	A vulnerability was found in TrueConf Server 4.3.7 and classified as problematic. This issue affects some unknown processing of the file /admin/conferences/list/. The manipulation of the argument sort leads to basic cross site scripting (Reflected). The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2017-20122	A vulnerability classified as problematic was found in Bitrix Site Manager 12.06.2015. Affected by this vulnerability is an unknown functionality of the component Contact Form. The manipulation of the argument text with the input leads to basic cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2017-20114	A vulnerability has been found in TrueConf Server 4.3.7 and classified as problematic. This vulnerability affects unknown code of the file /admin/conferences/get-all-status/. The manipulation of the argument keys[] leads to basic cross site scripting (Reflected). The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2017-20113	A vulnerability, which was classified as problematic, was found in TrueConf Server 4.3.7. This affects an unknown part. The manipulation leads to basic cross site scripting (Stored). It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2017-20119	A vulnerability classified as problematic has been found in TrueConf Server 4.3.7. This affects an unknown part of the file /admin/general/change-lang. The manipulation of the argument redirect_url leads to open redirect. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2022-2270	An issue has been discovered in GitLab affecting all versions starting from 12.4 before 14.10.5, all versions starting from 15.0 before 15.0.4, all versions starting from 15.1 before 15.1.1. GitLab was leaking Conan packages names due to incorrect permissions verification.	3.5	More Details
CVE-2022-34894	In JetBrains Hub before 2022.2.14799, insufficient access control allowed the hijacking of untrusted services	3.5	More Details
CVE-2017-20108	A vulnerability classified as problematic has been found in Easy Table Plugin 1.6. This affects an unknown part of the file /wordpress/wp-admin/options-general.php. The manipulation with the input "><script>alert(1)</script> leads to basic cross site scripting. It is possible to initiate the attack remotely.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1999	An issue has been discovered in GitLab CE/EE affecting all versions from 8.13 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1. Under certain conditions, using the REST API an unprivileged user was able to change labels description.	3.1	More Details
CVE-2022-2227	Improper access control in the runner jobs API in GitLab CE/EE affecting all versions prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows a previous maintainer of a project with a specific runner to access job and project meta data under certain conditions	3.1	More Details
CVE-2022-0167	An issue has been discovered in GitLab affecting all versions starting from 14.0 before 14.4.5, all versions starting from 14.5.0 before 14.5.3, all versions starting from 14.6.0 before 14.6.2. GitLab was not disabling the Autocomplete attribute of fields related to sensitive information making it possible to be retrieved under certain conditions.	3.1	More Details
CVE-2022-1981	An issue has been discovered in GitLab EE affecting all versions starting from 12.2 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1. In GitLab, if a group enables the setting to restrict access to users belonging to specific domains, that allow-list may be bypassed if a Maintainer uses the 'Invite a group' feature to invite a group that has members that don't comply with domain allow-list.	2.7	More Details
CVE-2022-2281	An information disclosure vulnerability in GitLab EE affecting all versions from 12.5 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows disclosure of release titles if group milestones are associated with any project releases.	2.6	More Details
CVE-2013-6498	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2013. Notes: none	N/A	More Details
CVE-2013-6471	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2013. Notes: none	N/A	More Details
CVE-2013-6464	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2013. Notes: none	N/A	More Details
CVE-2013-5683	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2013. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2013-6423	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2013. Notes: none	N/A	More Details
CVE-2013-6390	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2013. Notes: none	N/A	More Details
CVE-2013-7253	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2013. Notes: none	N/A	More Details
CVE-2013-4456	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2013. Notes: none	N/A	More Details
CVE-2013-4586	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2013. Notes: none	N/A	More Details
CVE-2013-4585	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2013. Notes: none	N/A	More Details
CVE-2013-2235	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA	N/A	More Details
CVE-2013-4506	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2013. Notes: none	N/A	More Details
CVE-2013-2252	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA	N/A	More Details
CVE-2013-4126	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-2013-4146	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2012-3414. Reason: This candidate is a duplicate of CVE-2012-3414. Notes: All CVE users should reference CVE-2012-3414 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2013-4493	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2013. Notes: none	N/A	More Details
CVE-2013-4309	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA	N/A	More Details
CVE-2013-4464	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during CVE-2013-4464. Notes: none	N/A	More Details
CVE-2013-4323	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2013-4252	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2022-33014	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-2022-33015	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-2022-33016	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-2022-2282	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: This CVE has been rejected as it was incorrectly assigned. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details