SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 04 January 2023

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-43931	Out-of-bounds write vulnerability in Remote Desktop Functionality in Synology VPN Plus Server before 1.4.3-0534 and 1.4.4-0635 allows remote attackers to execute arbitrary commands via unspecified vectors.	10.0	More Details
CVE-2022-47121	Tenda A15 V15.13.07.13 was discovered to contain a stack overflow via the wepkey parameter at /goform/WifiBasicSet.	9.8	More Details
CVE-2022-4049	The WP User WordPress plugin through 7.0 does not properly sanitize and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by unauthenticated users.	9.8	More Details
CVE-2022-47122	Tenda A15 V15.13.07.13 was discovered to contain a stack overflow via the wrlPwd_5g parameter at /goform/WifiBasicSet.	9.8	More Details
CVE-2022-47123	Tenda A15 V15.13.07.13 was discovered to contain a stack overflow via the wepkey3 parameter at /goform/WifiBasicSet.	9.8	More Details
CVE-2022-47124	Tenda A15 V15.13.07.13 was discovered to contain a stack overflow via the wepkey4 parameter at /goform/WifiBasicSet.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47125	Tenda A15 V15.13.07.13 was discovered to contain a stack overflow via the wrlEn_5g parameter at /goform/WifiBasicSet.	9.8	More Details
CVE-2022-47126	Tenda A15 V15.13.07.13 was discovered to contain a stack overflow via the wrlEn parameter at /goform/WifiBasicSet.	9.8	More Details
CVE-2022-47127	Tenda A15 V15.13.07.13 was discovered to contain a stack overflow via the wrlPwd parameter at /goform/WifiBasicSet.	9.8	More Details
CVE-2022-47128	Tenda A15 V15.13.07.13 was discovered to contain a stack overflow via the wepkey2 parameter at /goform/WifiBasicSet.	9.8	More Details
CVE-2022-48195	An issue was discovered in Mellium mellium.im/sasl before 0.3.1. When performing SCRAM-based SASL authentication, if the remote end advertises support for channel binding, no random nonce is generated (instead, the nonce is empty). This causes authentication to fail in the best case, but (if paired with a remote end that does not validate the length of the nonce) could lead to insufficient randomness being used during authentication.	9.8	More Details
CVE-2022-48198	The ntpd_driver component before 1.3.0 and 2.x before 2.2.0 for Robot Operating System (ROS) allows attackers, who control the source code of a different node in the same ROS application, to change a robot's behavior. This occurs because a topic name depends on the attacker-controlled time_ref_topic parameter.	9.8	More Details
CVE-2022-42475	A heap-based buffer overflow vulnerability [CWE-122] in FortiOS SSL-VPN 7.2.0 through 7.2.2, 7.0.0 through 7.0.8, 6.4.0 through 6.4.10, 6.2.0 through 6.2.11, 6.0.15 and earlier and FortiProxy SSL-VPN 7.2.0 through 7.2.1, 7.0.7 and earlier may allow a remote unauthenticated attacker to execute arbitrary code or commands via specifically crafted requests.	9.8	More Details
CVE-2022-3241	The Build App Online WordPress plugin before 1.0.19 does not properly sanitise and escape some parameters before using them in a SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection	9.8	More Details
CVE-2022-4059	The Cryptocurrency Widgets Pack WordPress plugin before 2.0 does not sanitise and escape some parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection.	9.8	More Details
CVE-2022-47119	Tenda A15 V15.13.07.13 was discovered to contain a stack overflow via the ssid parameter at /goform/WifiBasicSet.	9.8	More Details
CVE-2022-4099	The Joy Of Text Lite WordPress plugin before 2.3.1 does not properly sanitise and escape some parameters before using them in SQL statements accessible to unauthenticated users, leading to unauthenticated SQL injection	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4297	The WP AutoComplete Search WordPress plugin through 1.0.4 does not sanitise and escape a parameter before using it in a SQL statement via an AJAX available to unauthenticated users, leading to an unauthenticated SQL injection	9.8	More Details
CVE-2022-4298	The Wholesale Market WordPress plugin before 2.2.1 does not have authorisation check, as well as does not validate user input used to generate system path, allowing unauthenticated attackers to download arbitrary file from the server.	9.8	More Details
CVE-2022-4357	The LetsRecover WordPress plugin before 1.2.0 does not properly sanitise and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection.	9.8	More Details
CVE-2022-39039	aEnrich's a+HRD has inadequate filtering for specific URL parameter. An unauthenticated remote attacker can exploit this vulnerability to send arbitrary HTTP(s) request to launch Server-Side Request Forgery (SSRF) attack, to perform arbitrary system command or disrupt service.	9.8	More Details
CVE-2022-39041	aEnrich a+HRD has insufficient user input validation for specific API parameter. An unauthenticated remote attacker can exploit this vulnerability to inject arbitrary SQL commands to access, modify and delete database.	9.8	More Details
CVE-2022-39042	aEnrich a+HRD has improper validation for login function. An unauthenticated remote attacker can exploit this vulnerability to bypass authentication and access API function to perform arbitrary system command or disrupt service.	9.8	More Details
CVE-2022-47618	Merit LILIN AH55B04 & AH55B08 DVR firm has hard-coded administrator credentials. An unauthenticated remote attacker can use these credentials to log in administrator page, to manipulate system or disrupt service.	9.8	More Details
CVE-2021-32824	Apache Dubbo is a java based, open source RPC framework. Versions prior to 2.6.10 and 2.7.10 are vulnerable to pre-auth remote code execution via arbitrary bean manipulation in the Telnet handler. The Dubbo main service port can be used to access a Telnet Handler which offers some basic methods to collect information about the providers and methods exposed by the service and it can even allow to shutdown the service. This endpoint is unprotected. Additionally, a provider method can be invoked using the `invoke` handler. This handler uses a safe version of FastJson to process the call arguments. However, the resulting list is later processed with `PojoUtils.realize` which can be used to instantiate arbitrary classes and invoke its setters. Even though FastJson is properly protected with a default blocklist, `PojoUtils.realize` is not, and an attacker can leverage that to achieve remote code execution. Versions 2.6.10 and 2.7.10 contain fixes for this issue.	9.8	More Details
CVE-2022-32665	In Boa, there is a possible command injection due to improper input validation. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: A20220026; Issue ID: OSBNB00144124.	9.8	More Details
CVE-2022-47120	Tenda A15 V15.13.07.13 was discovered to contain a stack overflow via the security_5g parameter at /goform/WifiBasicSet.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38627	Nortek Linear eMerge E3-Series 0.32-08f, 0.32-07p, 0.32-07e, 0.32-09c, 0.32-09b, 0.32-09a, and 0.32-08e were discovered to contain a SQL injection vulnerability via the idt parameter.	9.8	More Details
CVE-2022-47118	Tenda A15 V15.13.07.13 was discovered to contain a stack overflow via the wepkey1 parameter at /goform/WifiBasicSet.	9.8	More Details
CVE-2022-46593	TRENDnet TEW755AP 1.13B01 was discovered to contain a stack overflow via the wps_sta_enrollee_pin parameter in the do_sta_enrollee_wifi function.	9.8	More Details
CVE-2022-44621	Diagnosis Controller miss parameter validation, so user may attacked by command injection via HTTP Request.	9.8	More Details
CVE-2022-46580	TRENDnet TEW755AP 1.13B01 was discovered to contain a stack overflow via the user_edit_page parameter in the wifi_captive_portal function.	9.8	More Details
CVE-2022-46581	TRENDnet TEW755AP 1.13B01 was discovered to contain a stack overflow via the cameo.cameo.nslookup_target parameter in the tools_nslookup function.	9.8	More Details
CVE-2022-46582	TRENDnet TEW755AP 1.13B01 was discovered to contain a stack overflow via the login_name parameter in the do_graph_auth (sub_4061E0) function.	9.8	More Details
CVE-2022-46583	TRENDnet TEW755AP 1.13B01 was discovered to contain a stack overflow via the reboot_type parameter in the wizard_ipv6 (sub_41C380) function.	9.8	More Details
CVE-2022-46584	TRENDnet TEW755AP 1.13B01 was discovered to contain a stack overflow via the qcawifi.wifi%d_vap%d.maclist parameter in the kick_ban_wifi_mac_deny (sub_415D7C) function.	9.8	More Details
CVE-2022-46585	TRENDnet TEW755AP 1.13B01 was discovered to contain a stack overflow via the REMOTE_USER parameter in the get_access (sub_45AC2C) function.	9.8	More Details
CVE-2022-46586	TRENDnet TEW755AP 1.13B01 was discovered to contain a stack overflow via the qcawifi.wifi%d_vap%d.maclist parameter in the kick_ban_wifi_mac_allow (sub_415B00) function.	9.8	More Details
CVE-2022-46588	TRENDnet TEW755AP 1.13B01 was discovered to contain a stack overflow via the sys_service parameter in the setup_wizard_mydlink (sub_4104B8) function.	9.8	More Details
CVE-2022-46589	TRENDnet TEW755AP 1.13B01 was discovered to contain a stack overflow via the cameo.cameo.netstat_option parameter in the tools_netstat (sub_41E730) function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46590	TRENDnet TEW755AP 1.13B01 was discovered to contain a stack overflow via the cameo.cameo.netstat_rsname parameter in the tools_netstat (sub_41E730) function.	9.8	More Details
CVE-2022-46591	TRENDnet TEW755AP 1.13B01 was discovered to contain a stack overflow via the reject_url parameter in the reject (sub_41BD60) function.	9.8	More Details
CVE-2022-46592	TRENDnet TEW755AP 1.13B01 was discovered to contain a stack overflow via the wps_sta_enrollee_pin parameter in the set_sta_enrollee_pin_5g function.	9.8	More Details
CVE-2022-46594	TRENDnet TEW755AP 1.13B01 was discovered to contain a stack overflow via the update_file_name parameter in the auto_up_fw (sub_420A04) function.	9.8	More Details
CVE-2022-46596	TRENDnet TEW755AP 1.13B01 was discovered to contain a stack overflow via the del_num parameter in the icp_delete_img (sub_41DEDC) function.	9.8	More Details
CVE-2022-46597	TRENDnet TEW755AP 1.13B01 was discovered to contain a command injection vulnerability via the sys_service parameter in the setup_wizard_mydlink (sub_4104B8) function.	9.8	More Details
CVE-2022-46598	TRENDnet TEW755AP 1.13B01 was discovered to contain a command injection vulnerability via the wps_sta_enrollee_pin parameter in the action set_sta_enrollee_pin_5g function.	9.8	More Details
CVE-2022-46599	TRENDnet TEW755AP 1.13B01 was discovered to contain a stack overflow via the setlogo_num parameter in the icp_setlogo_img (sub_41DBF4) function.	9.8	More Details
CVE-2022-46600	TRENDnet TEW755AP 1.13B01 was discovered to contain a stack overflow via the wps_sta_enrollee_pin parameter in the action set_sta_enrollee_pin_24g function.	9.8	More Details
CVE-2022-46601	TRENDnet TEW755AP 1.13B01 was discovered to contain a stack overflow via the setbg_num parameter in the icp_setbg_img (sub_41DD68) function.	9.8	More Details
CVE-2022-47115	Tenda A15 V15.13.07.13 was discovered to contain a stack overflow via the wepauth parameter at /goform/WifiBasicSet.	9.8	More Details
CVE-2022-47117	Tenda A15 V15.13.07.13 was discovered to contain a stack overflow via the security parameter at /goform/WifiBasicSet.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23555	authentik is an open-source Identity Provider focused on flexibility and versatility. Versions prior to 2022.11.4 and 2022.10.4 are vulnerable to Improper Authentication. Token reuse in invitation URLs leads to access control bypass via the use of a different enrollment flow than in the one provided. The vulnerability allows an attacker that knows different invitation flows names (e.g. `enrollment-invitation-test` and `enrollment-invitation-admin`) via either different invite links or via brute forcing to signup via a single invitation url for any valid invite link received (it can even be a url for a third flow as long as it's a valid invite) as the token used in the `Invitations` section of the Admin interface does NOT change when a different `enrollment flow` is selected via the interface and it is NOT bound to the selected flow, so it will be valid for any flow when used. This issue is patched in authentik 2022.11.4,2022.10.4 and 2022.12.0. Only configurations that use invitations and have multiple enrollment flows with invitation stages that grant different permissions are affected. The default configuration is not vulnerable, and neither are configurations with a single enrollment flow. As a workaround, fixed data can be added to invitations which can be checked in the flow to deny requests. Alternatively, an identifier with high entropy (like a UUID) can be used as flow slug, mitigating the attack vector by exponentially decreasing the possibility of discovering other flows.	9.4	More Details
CVE-2022-46179	LiuOS is a small Python project meant to imitate the functions of a regular operating system. Version 0.1.0 and prior of LiuOS allow an attacker to set the GITHUB_ACTIONS environment variable to anything other than null or true and skip authentication checks. This issue is patched in the latest commit (c658b4f3e57258acf5f6207a90c2f2169698ae22) by requiring the var to be set to true, causing a test script to run instead of being able to login. A potential workaround is to check for the GITHUB_ACTIONS environment variable and set it to "" (no quotes) to null the variable and force credential checks.	9.2	More Details
CVE-2022-36437	The Connection handler in Hazelcast and Hazelcast Jet allows a remote unauthenticated attacker to access and manipulate data in the cluster with the identity of another already authenticated connection. The affected Hazelcast versions are through 4.0.6, 4.1.9, 4.2.5, 5.0.3, and 5.1.2. The affected Hazelcast Jet versions are through 4.5.3.	9.1	More Details
CVE-2022-34322	Multiple XSS issues were discovered in Sage Enterprise Intelligence 2021 R1.1 that allow an attacker to execute JavaScript code in the context of users' browsers. The attacker needs to be authenticated to reach the vulnerable features. An issue is present in the Notify Users About Modification menu and the Notifications feature. A user can send malicious notifications and execute JavaScript code in the browser of every user who has enabled notifications. This is a stored XSS, and can lead to privilege escalation in the context of the application. (Another issue is present in the Favorites tab. The name of a favorite or a folder of favorites is interpreted as HTML, and can thus embed JavaScript code, which is executed when displayed. This is a self-XSS.)	9.0	More Details
CVE-2022-4866	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.9.1.	9.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4865	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.9.1.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-43396	In the fix for CVE-2022-24697, a blacklist is used to filter user input commands. But there is a risk of being bypassed. The user can control the command by controlling the kylin.engine.spark-cmd parameter of conf.	8.8	More Details
CVE-2022-43437	The Download function's parameter of EasyTest has insufficient validation for user input. A remote attacker authenticated as a general user can inject arbitrary SQL command to access, modify or delete database.	8.8	More Details
CVE-2022-4809	Improper Access Control in GitHub repository usememos/memos prior to 0.9.1.	8.8	More Details
CVE-2022-39947	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiADC version 7.0.0 through 7.0.2, FortiADC version 6.2.0 through 6.2.3, FortiADC version version 6.1.0 through 6.1.6, FortiADC version 6.0.0 through 6.0.4, FortiADC version 5.4.0 through 5.4.5 may allow an attacker to execute unauthorized code or commands via specifically crafted HTTP requests.	8.8	More Details
CVE-2022-4844	Cross-Site Request Forgery (CSRF) in GitHub repository usememos/memos prior to 0.9.1.	8.8	More Details
CVE-2022-48194	TP-Link TL-WR902AC devices through V3 0.9.1 allow remote authenticated attackers to execute arbitrary code or cause a Denial of Service (DoS) by uploading a crafted firmware update because the signature check is inadequate.	8.8	More Details
CVE-2022-46306	ChangingTec ServiSign component has a path traversal vulnerability due to insufficient filtering for special characters in the DLL file path. An unauthenticated remote attacker can host a malicious website for the component user to access, which triggers the component to load malicious DLL files under arbitrary file path and allows the attacker to perform arbitrary system operation and disrupt of service.	8.8	More Details
CVE-2022-46304	ChangingTec ServiSign component has insufficient filtering for special characters in the connection response parameter. An unauthenticated remote attacker can host a malicious website for the component user to access, which triggers command injection and allows the attacker to execute arbitrary system command to perform arbitrary system operation or disrupt service.	8.8	More Details
CVE-2022-43438	The Administrator function of EasyTest has an Incorrect Authorization vulnerability. A remote attacker authenticated as a general user can exploit this vulnerability to bypass the intended access restrictions, to make API functions calls, manipulate system and terminate service.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43436	The File Upload function of EasyTest has insufficient filtering for special characters and file type. A remote attacker authenticated as a general user can upload and execute arbitrary files, to manipulate system or disrupt service.	8.8	More Details
CVE-2022-4803	Authorization Bypass Through User-Controlled Key in GitHub repository usememos/memos prior to 0.9.1.	8.8	More Details
CVE-2022-2743	Integer overflow in Window Manager in Google Chrome on Chrome OS and Lacros prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific UI interactions to perform an out of bounds memory write via crafted UI interactions. (Chrome security severity: High)	8.8	More Details
CVE-2022-2742	Use after free in Exosphere in Google Chrome on Chrome OS and Lacros prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via crafted UI interactions. (Chrome security severity: High)	8.8	More Details
CVE-2021-30558	Insufficient policy enforcement in content security policy in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chrome security severity: Medium)	8.8	More Details
CVE-2022-4237	The Welcart e-Commerce WordPress plugin before 2.8.6 does not validate user input before using it in file_exist() functions via various AJAX actions available to any authenticated users, which could allow users with a role as low as subscriber to perform PHAR deserialisation when they can upload a file and a suitable gadget chain is present on the blog	8.8	More Details
CVE-2022-3911	The iubenda WordPress plugin before 3.3.3 does does not have authorisation and CSRF in an AJAX action, and does not ensure that the options to be updated belong to the plugin as long as they are arrays. As a result, any authenticated users, such as subscriber can grant themselves any privileges, such as edit_plugins etc	8.8	More Details
CVE-2022-3860	The Visual Email Designer for WooCommerce WordPress plugin before 1.7.2 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as author.	8.8	More Details
CVE-2022-34324	Multiple SQL injections in Sage XRT Business Exchange 12.4.302 allow an authenticated attacker to inject malicious data in SQL queries: Add Currencies, Payment Order, and Transfer History.	8.8	More Details
CVE-2022-4808	Improper Privilege Management in GitHub repository usememos/memos prior to 0.9.1.	8.8	More Details
CVE-2022-34669	NVIDIA GPU Display Driver for Windows contains a vulnerability in the user mode layer, where an unprivileged regular user can access or modify system files or other files that are critical to the application, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32664	In Config Manager, there is a possible command injection due to improper input validation. This could lead to remote escalation of privilege with User execution privileges needed. User interaction is needed for exploitation. Patch ID: A20220004; Issue ID: OSBNB00140929.	8.8	More Details
CVE-2022-38205	In some non-default installations of Esri Portal for ArcGIS versions 10.9.1 and below, a directory traversal issue may allow a remote, unauthenticated attacker to traverse the file system and lead to the disclosure of sensitive data (not customer-published content).	8.6	More Details
CVE-2022-38723	Gravitee API Management before 3.15.13 allows path traversal through HTML injection.	8.6	More Details
CVE-2022-34671	NVIDIA GPU Display Driver for Windows contains a vulnerability in the user-mode layer, where an unprivileged user can cause an out-of-bounds write, which may lead to code execution, information disclosure, and denial of service.	8.5	More Details
CVE-2022-4811	Authorization Bypass Through User-Controlled Key vulnerability in usememos usememos/memos.This issue affects usememos/memos before 0.9.1.	8.3	More Details
CVE-2022-41966	XStream serializes Java objects to XML and back again. Versions prior to 1.4.20 may allow a remote attacker to terminate the application with a stack overflow error, resulting in a denial of service only via manipulation the processed input stream. The attack uses the hash code implementation for collections and maps to force recursive hash calculation causing a stack overflow. This issue is patched in version 1.4.20 which handles the stack overflow and raises an InputManipulationException instead. A potential workaround for users who only use HashMap or HashSet and whose XML refers these only as default map or set, is to change the default implementation of java.util.Map and java.util per the code example in the referenced advisory. However, this implies that your application does not care about the implementation of the map and all elements are comparable.	8.2	More Details
CVE-2022-47634	M-Link Archive Server in Isode M-Link R16.2v1 through R17.0 before R17.0v24 allows non-administrative users to access and manipulate archive data via certain HTTP endpoints, aka LINK-2867.	8.1	More Details
CVE-2022-36943	SSZipArchive versions 2.5.3 and older contain an arbitrary file write vulnerability due to lack of sanitization on paths which are symlinks. SSZipArchive will overwrite files on the filesystem when opening a malicious ZIP containing a symlink as the first item.	8.1	More Details
CVE-2022-38766	The remote keyless system on Renault ZOE 2021 vehicles sends 433.92 MHz RF signals from the same Rolling Codes set for each door-open request, which allows for a replay attack.	8.1	More Details
CVE-2022-4796	Incorrect Use of Privileged APIs in GitHub repository usememos/memos prior to 0.9.1.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42269	NVIDIA Trusted OS contains a vulnerability in an SMC call handler, where failure to validate untrusted input may allow a highly privileged local attacker to cause information disclosure and compromise integrity. The scope of the impact can extend to other components.	7.9	More Details
CVE-2022-35845	Multiple improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in FortiTester 7.1.0, 7.0 all versions, 4.0.0 through 4.2.0, 2.3.0 through 3.9.1 may allow an authenticated attacker to execute arbitrary commands in the underlying shell.	7.8	More Details
CVE-2022-32635	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573237.	7.8	More Details
CVE-2022-43448	Out-of-bounds write vulnerability in V-SFT v6.1.7.0 and earlier and TELLUS v4.0.12.0 and earlier allows a local attacker to obtain the information and/or execute arbitrary code by having a user to open a specially crafted image file.	7.8	More Details
CVE-2022-47908	Stack-based buffer overflow vulnerability in V-Server v4.0.12.0 and earlier allows a local attacker to obtain the information and/or execute arbitrary code by having a user to open a specially crafted project file.	7.8	More Details
CVE-2022-46360	Out-of-bounds read vulnerability in V-SFT v6.1.7.0 and earlier and TELLUS v4.0.12.0 and earlier allows a local attacker to obtain the information and/or execute arbitrary code by having a user to open a specially crafted image file.	7.8	More Details
CVE-2022-47317	Out-of-bounds write vulnerability in V-Server v4.0.12.0 and earlier allows a local attacker to obtain the information and/or execute arbitrary code by having a user to open a specially crafted project file.	7.8	More Details
CVE-2022-44564	Huawei Aslan Children's Watch has a path traversal vulnerability. Successful exploitation may allow attackers to access or modify protected system resources.	7.8	More Details
CVE-2022-41645	Out-of-bounds read vulnerability in V-Server v4.0.12.0 and earlier allows a local attacker to obtain the information and/or execute arbitrary code by having a user to open a specially crafted project file.	7.8	More Details
CVE-2022-42261	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where an input index is not validated, which may lead to buffer overrun, which in turn may cause data tampering, information disclosure, or denial of service.	7.8	More Details
CVE-2022-42260	NVIDIA vGPU Display Driver for Linux guest contains a vulnerability in a D-Bus configuration file, where an unauthorized user in the guest VM can impact protected D-Bus endpoints, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.	7.8	More Details
CVE-2022-34670	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer handler, where an unprivileged regular user can cause truncation errors when casting a primitive to a primitive of smaller size causes data to be lost in the conversion, which may lead to denial of service or information disclosure.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34672	NVIDIA Control Panel for Windows contains a vulnerability where an unauthorized user or an unprivileged regular user can compromise the security of the software by gaining privileges, reading sensitive information, or executing commands.	7.8	More Details
CVE-2022-42270	NVIDIA distributions of Linux contain a vulnerability in nvdla_emu_task_submit, where unvalidated input may allow a local attacker to cause stack-based buffer overflow in kernel code, which may lead to escalation of privileges, compromised integrity and confidentiality, and denial of service.	7.8	More Details
CVE-2022-47116	Tenda A15 V15.13.07.13 was discovered to contain a stack overflow via the SYSPS parameter at /goform/SysToolChangePwd.	7.5	More Details
CVE-2022-4779	StreamX applications from versions 6.02.01 to 6.04.34 are affected by a logic bug that allows to bypass the implemented authentication scheme. StreamX applications using StreamView HTML component with the public web server feature activated are affected.	7.5	More Details
CVE-2022-3842	Use after free in Passwords in Google Chrome prior to 105.0.5195.125 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2022-3347	DNSSEC validation is not performed correctly. An attacker can cause this package to report successful validation for invalid, attacker-controlled records. Root DNSSEC public keys are not validated, permitting an attacker to present a self-signed root key and delegation chain.	7.5	More Details
CVE-2022-39040	aEnrich a+HRD log read function has a path traversal vulnerability. An unauthenticated remote attacker can exploit this vulnerability to bypass authentication and download arbitrary system files.	7.5	More Details
CVE-2022-38203	Protections against potential Server-Side Request Forgery (SSRF) vulnerabilities in Esri Portal for ArcGIS versions 10.8.1 and below were not fully honored and may allow a remote, unauthenticated attacker to forge requests to arbitrary URLs from the system, potentially leading to network enumeration or reading from hosts inside the network perimeter, a different issue than CVE-2022-38211 and CVE-2022-38212.	7.5	More Details
CVE-2022-45143	The JsonErrorReportValve in Apache Tomcat 8.5.83, 9.0.40 to 9.0.68 and 10.1.0-M1 to 10.1.1 did not escape the type, message or description values. In some circumstances these are constructed from user provided data and it was therefore possible for users to supply values that invalidated or manipulated the JSON output.	7.5	More Details
CVE-2022-38212	Protections against potential Server-Side Request Forgery (SSRF) vulnerabilities in Esri Portal for ArcGIS versions 10.8.1 and below were not fully honored and may allow a remote, unauthenticated attacker to forge requests to arbitrary URLs from the system, potentially leading to network enumeration or reading from hosts inside the network perimeter, a different issue than CVE-2022-38211 and CVE-2022-38203.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38211	Protections against potential Server-Side Request Forgery (SSRF) vulnerabilities in Esri Portal for ArcGIS versions 10.9.1 and below were not fully honored and may allow a remote, unauthenticated attacker to forge requests to arbitrary URLs from the system, potentially leading to network enumeration or reading from hosts inside the network perimeter, a different issue than CVE-2022-38211 and CVE-2022-38212.	7.5	More Details
CVE-2022-3460	In affected versions of Octopus Deploy it is possible for certain types of sensitive variables to inadvertently become unmasked when viewed in variable preview.	7.5	More Details
CVE-2023-22551	The FTP (aka "Implementation of a simple FTP client and server") project through 96c1a35 allows remote attackers to cause a denial of service (memory consumption) by engaging in client activity, such as establishing and then terminating a connection. This occurs because malloc is used but free is not.	7.5	More Details
CVE-2022-23553	Alpine is a scaffolding library in Java. Alpine prior to version 1.10.4 allows URL access filter bypass. This issue has been fixed in version 1.10.4. There are no known workarounds.	7.5	More Details
CVE-2020-36562	Due to unchecked type assertions, maliciously crafted messages can cause panics, which may be used as a denial of service vector.	7.5	More Details
CVE-2022-4140	The Welcart e-Commerce WordPress plugin before 2.8.5 does not validate user input before using it to output the content of a file, which could allow unauthenticated attacker to read arbitrary files on the server	7.5	More Details
CVE-2022-4843	NULL Pointer Dereference in GitHub repository radareorg/radare2 prior to 5.8.2.	7.5	More Details
CVE-2022-39012	Huawei Aslan Children's Watch has an improper input validation vulnerability. Successful exploitation may cause the watch's application service abnormal.	7.5	More Details
CVE-2022-38202	There is a path traversal vulnerability in Esri ArcGIS Server versions 10.9.1 and below. Successful exploitation may allow a remote, unauthenticated attacker traverse the file system to access files outside of the intended directory on ArcGIS Server. This could lead to the disclosure of sensitive site configuration information (not user datasets).	7.5	More Details
CVE-2022-37785	An issue was discovered in WeCube Platform 3.2.2. Cleartext passwords are displayed in the configuration for terminal plugins.	7.5	More Details
CVE-2022-48196	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects RAX40 before 1.0.2.60, RAX35 before 1.0.2.60, R6400v2 before 1.0.4.122, R6700v3 before 1.0.4.122, R6900P before 1.3.3.152, R7000P before 1.3.3.152, R7000 before 1.0.11.136, R7960P before 1.4.4.94, and R8000P before 1.4.4.94.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-13768	Use after free in FileAPI in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chrome security severity: High)	7.4	More Details
CVE-2022-46178	MeterSphere is a one-stop open source continuous testing platform, covering test management, interface testing, UI testing and performance testing. Versions prior to 2.5.1 allow users to upload a file, but do not validate the file name, which may lead to upload file to any path. The vulnerability has been fixed in v2.5.1. There are no workarounds.	7.4	More Details
CVE-2022-4855	A vulnerability, which was classified as critical, was found in SourceCodester Lead Management System 1.0. Affected is an unknown function of the file login.php. The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-217020.	7.3	More Details
CVE-2022-44036	In b2evolution 7.2.5, if configured with admins_can_manipulate_sensitive_files, arbitrary file upload is allowed for admins, leading to command execution. NOTE: the vendor's position is that this is "very obviously a feature not an issue and if you don't like that feature it is very obvious how to disable it."	7.2	More Details
CVE-2022-44137	SourceCodester Sanitization Management System 1.0 is vulnerable to SQL Injection.	7.2	More Details
CVE-2022-46173	Elrond-GO is a go implementation for the Elrond Network protocol. Versions prior to 1.3.50 are subject to a processing issue where nodes are affected when trying to process a cross-shard relayed transaction with a smart contract deploy transaction data. The problem was a bad correlation between the transaction caches and the processing component. If the above-mentioned transaction was sent with more gas than required, the smart contract result (SCR transaction) that should have returned the leftover gas, would have been wrongly added to a cache that the processing unit did not consider. The node stopped notarizing metachain blocks. The fix was actually to extend the SCR transaction search in all other caches if it wasn't found in the correct (expected) sharded-cache. There are no known workarounds at this time. This issue has been patched in version 1.3.50.	7.2	More Details
CVE-2022-40740	Realtek GPON router has insufficient filtering for special characters. A remote attacker authenticated as an administrator can exploit this vulnerability to perform command injection attacks, to execute arbitrary system command, manipulate system or disrupt service.	7.2	More Details
CVE-2022-4373	The Quote-O-Matic WordPress plugin through 1.0.5 does not properly sanitize and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin.	7.2	More Details
CVE-2022-4372	The Web Invoice WordPress plugin through 2.1.3 does not properly sanitize and escape a parameter before using it in a SQL statement, leading to a SQL Injection exploitable by high privilege users such as admin by default. However, depending on the plugin configuration, other users, such as subscriber could exploit this as well	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4370	The multimedial images WordPress plugin through 1.0b does not properly sanitize and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as Admin.	7.2	More Details
CVE-2022-4360	The WP RSS By Publishers WordPress plugin through 0.1 does not properly sanitize and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin	7.2	More Details
CVE-2022-4359	The WP RSS By Publishers WordPress plugin through 0.1 does not properly sanitize and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin	7.2	More Details
CVE-2022-4358	The WP RSS By Publishers WordPress plugin through 0.1 does not properly sanitize and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin	7.2	More Details
CVE-2022-4356	The LetsRecover WordPress plugin before 1.2.0 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin	7.2	More Details
CVE-2022-4355	The LetsRecover WordPress plugin before 1.2.0 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin	7.2	More Details
CVE-2022-4352	The Qe SEO Handyman WordPress plugin through 1.0 does not properly sanitize and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin	7.2	More Details
CVE-2022-4351	The Qe SEO Handyman WordPress plugin through 1.0 does not properly sanitize and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin	7.2	More Details
CVE-2022-4324	The Custom Field Template WordPress plugin before 2.5.8 unserialises the content of an imported file, which could lead to PHP object injections issues when a high privilege user import (intentionally or not) a malicious Customizer Styling file and a suitable gadget chain is present on the blog.	7.2	More Details
CVE-2022-4302	The White Label CMS WordPress plugin before 2.5 unserializes user input provided via the settings, which could allow high-privilege users such as admin to perform PHP Object Injection when a suitable gadget is present.	7.2	More Details
CVE-2022-4371	The Web Invoice WordPress plugin through 2.1.3 does not properly sanitize and escape a parameter before using it in a SQL statement, leading to a SQL Injection exploitable by high privilege users such as admin by default. However, depending on the plugin configuration, other users, such as subscriber could exploit this as well	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23544	MeterSphere is a one-stop open source continuous testing platform, covering test management, interface testing, UI testing and performance testing. Versions prior to 2.5.0 are subject to a Server-Side Request Forgery that leads to Cross-Site Scripting. A Server-Side request forgery in `IssueProxyResourceService::getMdImageByUrl` allows an attacker to access internal resources, as well as executing JavaScript code in the context of Metersphere's origin by a victim of a reflected XSS. This vulnerability has been fixed in v2.5.0. There are no known workarounds.	7.2	More Details
CVE-2023-0038	The "Survey Maker – Best WordPress Survey Plugin" plugin for WordPress is vulnerable to Stored Cross-Site Scripting via survey answers in versions up to, and including, 3.1.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts when submitting quizzes that will execute whenever a user accesses the submissions page.	7.2	More Details
CVE-2022-45867	MyBB before 1.8.33 allows Directory Traversal. The Admin CP Languages module allows remote authenticated users, with high privileges, to achieve local file inclusion and execution.	7.2	More Details
CVE-2022-42262	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where an input index is not validated, which may lead to buffer overrun, which in turn may cause data tampering, information disclosure, or denial of service.	7.1	More Details
CVE-2022-34676	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer handler, where an out-of-bounds read may lead to denial of service, information disclosure, or data tampering.	7.1	More Details
CVE-2022-42264	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where an unprivileged regular user can cause the use of an out-of-range pointer offset, which may lead to data tampering, data loss, information disclosure, or denial of service.	7.1	More Details
CVE-2022-42263	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer handler, where an Integer overflow may lead to denial of service or information disclosure.	7.1	More Details
CVE-2022-41967	Dragonfly is a Java runtime dependency management library. Dragonfly v0.3.0-SNAPSHOT does not configure DocumentBuilderFactory to prevent XML external entity (XXE) attacks. This issue is patched in 0.3.1-SNAPSHOT. As a workaround, since Dragonfly only parses XML `SNAPSHOT` versions are being resolved, this vulnerability may be avoided by not trying to resolve `SNAPSHOT` versions.	7.0	More Details
CVE-2022-42267	NVIDIA GPU Display Driver for Windows contains a vulnerability where a regular user can cause an out-of-bounds read, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.	7.0	More Details
CVE-2022-41336	An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiPortal versions 6.0.0 through 6.0.11 and all versions of 5.3, 5.2, 5.1, 5.0 management interface may allow a remote authenticated attacker to perform a stored cross site scripting (XSS) attack via sending request with specially crafted columnindex parameter.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34674	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer handler, where a helper function maps more physical pages than were requested, which may lead to undefined behavior or an information leak.	6.8	More Details
CVE-2022-32657	In Wi-Fi driver, there is a possible undefined behavior due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220705042; Issue ID: GN20220705042.	6.7	More Details
CVE-2022-32652	In mtk-aie, there is a possible use after free due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07262617; Issue ID: ALPS07262617.	6.7	More Details
CVE-2022-32651	In mtk-aie, there is a possible use after free due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07225857; Issue ID: ALPS07225857.	6.7	More Details
CVE-2022-32636	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07510064.	6.7	More Details
CVE-2022-32623	In mdp, there is a possible out of bounds write due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07342114; Issue ID: ALPS07342114.	6.7	More Details
CVE-2022-32637	In hevc decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07491374; Issue ID: ALPS07491374.	6.7	More Details
CVE-2022-32653	In mtk-aie, there is a possible use after free due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07262518; Issue ID: ALPS07262518.	6.7	More Details
CVE-2022-32649	In jpeg, there is a possible use after free due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07225840; Issue ID: ALPS07225840.	6.7	More Details
CVE-2022-32641	In meta wifi, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453594; Issue ID: ALPS07453594.	6.7	More Details
CVE-2022-32640	In meta wifi, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441652; Issue ID: ALPS07441652.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32650	In mtk-isp, there is a possible use after free due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07225853; Issue ID: ALPS07225853.	6.7	More Details
CVE-2022-32659	In Wi-Fi driver, there is a possible undefined behavior due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220705066; Issue ID: GN20220705066.	6.7	More Details
CVE-2022-32646	In gpu drm, there is a possible stack overflow due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363501; Issue ID: ALPS07363501.	6.7	More Details
CVE-2022-32658	In Wi-Fi driver, there is a possible undefined behavior due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220705059; Issue ID: GN20220705059.	6.7	More Details
CVE-2022-32647	In ccu, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07554646; Issue ID: ALPS07554646.	6.7	More Details
CVE-2023-22451	Kiwi TCMS is an open source test management system. In version 11.6 and prior, when users register new accounts and/or change passwords, there is no validation in place which would prevent them from picking an easy to guess password. This issue is resolved by providing defaults for the `AUTH_PASSWORD_VALIDATORS` configuration setting. As of version 11.7, the password can’t be too similar to other personal information, must contain at least 10 characters, can’t be a commonly used password, and can’t be entirely numeric. As a workaround, an administrator may reset all passwords in Kiwi TCMS if they think a weak password may have been chosen.	6.5	More Details
CVE-2023-22452	kenny2automate is a Discord bot. In the web interface for server settings, form elements were generated with Discord channel IDs as part of input names. Prior to commit a947d7c, no validation was performed to ensure that the channel IDs submitted actually belonged to the server being configured. Thus anyone who has access to the channel ID they wish to change settings for and the server settings panel for any server could change settings for the requested channel no matter which server it belonged to. Commit a947d7c resolves the issue and has been deployed to the official instance of the bot. The only workaround that exists is to disable the web config entirely by changing it to run on localhost. Note that a workaround is only necessary for those who run their own instance of the bot.	6.5	More Details
CVE-2022-4800	Improper Verification of Source of a Communication Channel in GitHub repository usememos/memos prior to 0.9.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4236	The Welcart e-Commerce WordPress plugin before 2.8.5 does not validate user input before using it to output the content of a file via an AJAX action available to any authenticated users, which could allow users with a role as low as subscriber to read arbitrary files on the server.	6.5	More Details
CVE-2022-34678	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where an unprivileged user can cause a null-pointer dereference, which may lead to denial of service.	6.5	More Details
CVE-2022-4812	Authorization Bypass Through User-Controlled Key in GitHub repository usememos/memos prior to 0.9.1.	6.5	More Details
CVE-2022-4799	Authorization Bypass Through User-Controlled Key in GitHub repository usememos/memos prior to 0.9.1.	6.5	More Details
CVE-2022-41579	There is an insufficient authentication vulnerability in some Huawei band products. Successful exploit could allow the attacker to spoof then connect to the band.	6.5	More Details
CVE-2022-46740	There is a denial of service vulnerability in the Wi-Fi module of the HUAWEI WS7100-20 Smart WiFi Router.Successful exploit could cause a denial of service (DoS) condition.	6.5	More Details
CVE-2022-23554	Alpine is a scaffolding library in Java. Alpine prior to version 1.10.4 allows Authentication Filter bypass. The AuthenticationFilter relies on the request URI to evaluate if the user is accessing the swagger endpoint. By accessing a URL with a path such as /api/foo;%2fapi%2fswagger the contains condition will hold and will return from the authentication filter without aborting the request. Note that the principal object will not be assigned and therefore the issue wont allow user impersonation. This issue has been fixed in version 1.10.4. There are no known workarounds.	6.5	More Details
CVE-2022-2967	Prosys OPC UA Simulation Server version prior to v5.3.0-64 and UA Modbus Server versions 1.4.18-5 and prior do not sufficiently protect credentials, which could allow an attacker to obtain user credentials and gain access to system data.	6.5	More Details
CVE-2022-4778	StreamX applications from versions 6.02.01 to 6.04.34 are affected by a path traversal vulnerability that allows authenticated users to get unauthorized access to files on the server's filesystem. StreamX applications using StreamView HTML component with the public web server feature activated are affected.	6.5	More Details
CVE-2022-0337	Inappropriate implementation in File System API in Google Chrome on Windows prior to 97.0.4692.71 allowed a remote attacker to obtain potentially sensitive information via a crafted HTML page. (Chrome security severity: High)	6.5	More Details
CVE-2022-4847	Incorrectly Specified Destination in a Communication Channel in GitHub repository usememos/memos prior to 0.9.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4849	Cross-Site Request Forgery (CSRF) in GitHub repository usememos/memos prior to 0.9.1.	6.5	More Details
CVE-2022-4863	Improper Handling of Insufficient Permissions or Privileges in GitHub repository usememos/memos prior to 0.9.1.	6.5	More Details
CVE-2022-4850	Cross-Site Request Forgery (CSRF) in GitHub repository usememos/memos prior to 0.9.1.	6.5	More Details
CVE-2022-46305	ChangingTec ServiSign component has a path traversal vulnerability. An unauthenticated LAN attacker can exploit this vulnerability to bypass authentication and access arbitrary system files.	6.5	More Details
CVE-2022-46309	Vitals ESP upload function has a path traversal vulnerability. A remote attacker with general user privilege can exploit this vulnerability to access arbitrary system files.	6.5	More Details
CVE-2022-4846	Cross-Site Request Forgery (CSRF) in GitHub repository usememos/memos prior to 0.9.1.	6.5	More Details
CVE-2022-3346	DNSSEC validation is not performed correctly. An attacker can cause this package to report successful validation for invalid, attacker-controlled records. The owner name of RRSIG RRs is not validated, permitting an attacker to present the RRSIG for an attacker-controlled domain in a response for any other domain.	6.5	More Details
CVE-2022-46172	authentik is an open-source Identity provider focused on flexibility and versatility. In versions prior to 2022.10.4, and 2022.11.4, any authenticated user can create an arbitrary number of accounts through the default flows. This would circumvent any policy in a situation where it is undesirable for users to create new accounts by themselves. This may also affect other applications as these new basic accounts would exist throughout the SSO infrastructure. By default the newly created accounts cannot be logged into as no password reset exists by default. However password resets are likely to be enabled by most installations. This vulnerability pertains to the user context used in the default-user-settings-flow, /api/v3/flows/instances/default-user-settings-flow/execute/. This issue has been fixed in versions 2022.10.4 and 2022.11.4.	6.4	More Details
CVE-2022-32638	In isp, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494449; Issue ID: ALPS07494449.	6.4	More Details
CVE-2022-32648	In disp, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535964; Issue ID: ALPS06535964.	6.4	More Details
CVE-2022-32644	In vow, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494473; Issue ID: ALPS07494473.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2014-125030	A vulnerability, which was classified as critical, has been found in taoeffect Empress. Affected by this issue is some unknown functionality. The manipulation leads to use of hard-coded password. The patch is identified as 557e177d8a309d6f0f26de46efb38d43e000852d. It is recommended to apply a patch to fix this issue. VDB-217154 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-4856	A vulnerability has been found in Modbus Tools Modbus Slave up to 7.5.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file mbslave.exe of the component mbs File Handler. The manipulation leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-217021 was assigned to this vulnerability.	6.3	More Details
CVE-2022-4857	A vulnerability was found in Modbus Tools Modbus Poll up to 9.10.0 and classified as critical. Affected by this issue is some unknown functionality of the file mbpoll.exe of the component mbp File Handler. The manipulation leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-217022 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2015-10008	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in 82Flex WEIPDCRM. It has been classified as critical. This affects an unknown part. The manipulation leads to sql injection. It is possible to initiate the attack remotely. The identifier of the patch is 43bad79392332fa39e31b95268e76fbda9fec3a4. It is recommended to apply a patch to fix this issue. The identifier VDB-217185 was assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2017-20160	A vulnerability was found in flitto express-param up to 0.x. It has been classified as critical. This affects an unknown part of the file lib/fetchParams.js. The manipulation leads to improper handling of extra parameters. It is possible to initiate the attack remotely. Upgrading to version 1.0.0 is able to address this issue. The identifier of the patch is db94f7391ad0a16dcfcba8b9be1af385b25c42db. It is recommended to upgrade the affected component. The identifier VDB-217149 was assigned to this vulnerability.	6.3	More Details
CVE-2022-37786	An issue was discovered in WeCube Platform 3.2.2. There are multiple CSV injection issues: the [Home / Admin / Resources] page, the [Home / Admin / System Params] page, and the [Home / Design / Basekey Configuration] page.	6.3	More Details
CVE-2021-32821	MooTools is a collection of JavaScript utilities for JavaScript developers. All known versions include a CSS selector parser that is vulnerable to Regular Expression Denial of Service (ReDoS). An attack requires that an attacker can inject a string into a CSS selector at runtime, which is quite common with e.g. jQuery CSS selectors. No patches are available for this issue.	6.2	More Details
CVE-2022-38208	There is an unvalidated redirect vulnerability in Esri Portal for ArcGIS 11 and below that may allow a remote, unauthenticated attacker to craft a URL that could redirect a victim to an arbitrary website, simplifying phishing attacks.	6.1	More Details
CVE-2022-37787	An issue was discovered in WeCube platform 3.2.2. A DOM XSS vulnerability has been found on the plugin database execution page.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46181	Gotify server is a simple server for sending and receiving messages in real-time per WebSocket. Versions prior to 2.2.2 contain an XSS vulnerability that allows authenticated users to upload .html files. An attacker could execute client side scripts **if** another user opened a link. The attacker could potentially take over the account of the user that clicked the link. The Gotify UI won't natively expose such a malicious link, so an attacker has to get the user to open the malicious link in a context outside of Gotify. The vulnerability has been fixed in version 2.2.2. As a workaround, you can block access to non image files via a reverse proxy in the `./image` directory.	6.1	More Details
CVE-2022-38207	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 10.8.1 and 10.7.1 which may allow a remote remote, unauthenticated attacker to create a crafted link which when clicked which could execute arbitrary JavaScript code in the victim’s browser.	6.1	More Details
CVE-2021-41823	The Web Application Firewall (WAF) in Kemp LoadMaster 7.2.54.1 allows certain uses of onmouseover to bypass an XSS protection mechanism.	6.1	More Details
CVE-2022-38206	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 10.9.1 and below which may allow a remote remote, unauthenticated attacker to create a crafted link which when clicked could execute arbitrary JavaScript code in the victim’s browser.	6.1	More Details
CVE-2022-38204	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 10.8.1 and 10.7.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim’s browser.	6.1	More Details
CVE-2022-30519	XSS in signing form in Reprise Software RLM License Administration v14.2BL4 allows remote attacker to inject arbitrary code via password field.	6.1	More Details
CVE-2022-38209	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 10.9.1 and below which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could execute arbitrary JavaScript code in the victim’s browser.	6.1	More Details
CVE-2022-3863	Use after free in Browser History in Google Chrome prior to 100.0.4896.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chrome security severity: High)	6.1	More Details
CVE-2022-4369	The WP-Lister Lite for Amazon WordPress plugin before 2.4.4 does not sanitize and escapes a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which can be used against high-privilege users such as admin.	6.1	More Details
CVE-2022-38210	There is a reflected HTML injection vulnerability in Esri Portal for ArcGIS versions 10.9.1 and below that may allow a remote, unauthenticated attacker to create a crafted link which when clicked could render arbitrary HTML in the victim’s browser.	6.1	More Details
CVE-2022-4329	The Product list Widget for Woocommerce WordPress plugin through 1.0 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against both unauthenticated and authenticated users (such as high privilege one like admin).	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0801	Inappropriate implementation in HTML parser in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to bypass XSS preventions via a crafted HTML page. (Chrome security severity: Medium)	6.1	More Details
CVE-2022-3614	In affected versions of Octopus Deploy users of certain browsers using AD to sign-in to Octopus Server were able to bypass authentication checks and be redirected to the configured redirect url without any validation.	6.1	More Details
CVE-2022-48197	Reflected cross-site scripting (XSS) exists in Sandbox examples in the YUI2 repository. The download distributions, TreeView component and the YUI Javascript library overall are not affected. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	6.1	More Details
CVE-2023-22456	ViewVC, a browser interface for CVS and Subversion version control repositories, as a cross-site scripting vulnerability that affects versions prior to 1.2.2 and 1.1.29. The impact of this vulnerability is mitigated by the need for an attacker to have commit privileges to a Subversion repository exposed by an otherwise trusted ViewVC instance. The attack vector involves files with unsafe names (names that, when embedded into an HTML stream, would cause the browser to run unwanted code), which themselves can be challenging to create. Users should update to at least version 1.2.2 (if they are using a 1.2.x version of ViewVC) or 1.1.29 (if they are using a 1.1.x version). ViewVC 1.0.x is no longer supported, so users of that release lineage should implement a workaround. Users can edit their ViewVC EZT view templates to manually HTML-escape changed paths during rendering. Locate in your template set's `revision.ezt` file references to those changed paths, and wrap them with `[format "html"]` and `[end]`. For most users, that means that references to `[changes.path]` will become `[format "html"][changes.path][end]`. (This workaround should be reverted after upgrading to a patched version of ViewVC, else changed path names will be doubly escaped.)	6.1	More Details
CVE-2022-4848	Improper Verification of Source of a Communication Channel in GitHub repository usememos/memos prior to 0.9.1.	5.7	More Details
CVE-2023-0028	Cross-site Scripting (XSS) - Stored in GitHub repository linagora/twake prior to 2023.Q1.1200+.	5.7	More Details
CVE-2022-34677	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer handler, where an unprivileged regular user can cause an integer to be truncated, which may lead to denial of service or data tampering.	5.5	More Details
CVE-2022-34679	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer handler, where an unhandled return value can lead to a null-pointer dereference, which may lead to denial of service.	5.5	More Details
CVE-2022-34680	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer handler, where an integer truncation can lead to an out-of-bounds read, which may lead to denial of service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-20151	A vulnerability classified as problematic was found in iText RUPS. This vulnerability affects unknown code of the file src/main/java/com/itextpdf/rups/model/XfaFile.java. The manipulation leads to xml external entity reference. The patch is identified as ac5590925874ef810018a6b60fec216eee54fb32. It is recommended to apply a patch to fix this issue. VDB-217054 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2022-34682	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where an unprivileged regular user can cause a null-pointer dereference, which may lead to denial of service.	5.5	More Details
CVE-2022-34683	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a null-pointer dereference occurs, which may lead to denial of service.	5.5	More Details
CVE-2022-34675	NVIDIA Display Driver for Linux contains a vulnerability in the Virtual GPU Manager, where it does not check the return value from a null-pointer dereference, which may lead to denial of service.	5.5	More Details
CVE-2017-20150	A vulnerability was found in challenge website. It has been rated as critical. This issue affects some unknown processing. The manipulation leads to sql injection. The name of the patch is f1644b1d3502e5aa5284f31ea80d2623817f4d42. It is recommended to apply a patch to fix this issue. The identifier VDB-216989 was assigned to this vulnerability.	5.5	More Details
CVE-2022-45874	Huawei Aslan Children's Watch has an improper authorization vulnerability. Successful exploit could allow the attacker to access certain file.	5.5	More Details
CVE-2018-25057	A vulnerability was found in simple_php_link_shortener. It has been classified as critical. Affected is an unknown function of the file index.php. The manipulation of the argument $link["id"] leads to sql injection. The name of the patch is b26ac6480761635ed94ccb0222ba6b732de6e53f. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-216996.	5.5	More Details
CVE-2022-4818	A vulnerability was found in Talend Open Studio for MDM. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file org.talend.mdm.core/src/com/amalto/core/storage/SystemStorageWrapper.java. The manipulation leads to xml external entity reference. Upgrading to version 20221220_1938 is able to address this issue. The name of the patch is 95590db2ad6a582c371273ceab1a73ad6ed47853. It is recommended to upgrade the affected component. The identifier VDB-216997 was assigned to this vulnerability.	5.5	More Details
CVE-2022-34681	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler, where improper input validation of a display-related data structure may lead to denial of service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2015-10009	A vulnerability was found in nterchange up to 4.1.0. It has been rated as critical. This issue affects the function getContent of the file app/controllers/code_caller_controller.php. The manipulation of the argument q with the input %5C%27%29;phpinfo%28%29;/* leads to code injection. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.1 is able to address this issue. The patch is named fba7d89176fba8fe289edd58835fe45080797d99. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-217187.	5.5	More Details
CVE-2022-42266	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where an unprivileged regular user can cause exposure of sensitive information to an actor that is not explicitly authorized to have access to that information, which may lead to limited information disclosure.	5.5	More Details
CVE-2022-4860	A vulnerability was found in KBase Metrics. It has been classified as critical. This affects the function upload_user_data of the file source/daily_cron_jobs/methods_upload_user_stats.py. The manipulation leads to sql injection. The patch is named 959dfb6b05991e30b0fa972a1ecdcaae8e1dae6d. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217059.	5.5	More Details
CVE-2021-4298	A vulnerability classified as critical has been found in Hesburgh Libraries of Notre Dame Sipity. This affects the function SearchCriteriaForWorksParameter of the file app/parameters/sipity/parameters/search_criteria_for_works_parameter.rb. The manipulation leads to sql injection. Upgrading to version 2021.8 is able to address this issue. The patch is named d1704c7363b899ffce65be03a796a0ee5fdbfbdc. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-217179.	5.5	More Details
CVE-2014-125032	A vulnerability was found in porpeeranut go-with-me. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file module/frontend/add.php. The manipulation leads to sql injection. The identifier of the patch is b92451e4f9e85e26cf493c95ea0a69e354c35df9. It is recommended to apply a patch to fix this issue. The identifier VDB-217177 was assigned to this vulnerability.	5.5	More Details
CVE-2021-4297	A vulnerability has been found in trampgeek jobe up to 1.6.4 and classified as problematic. This vulnerability affects the function runs_post of the file application/controllers/Restapi.php. The manipulation of the argument sourcefilename leads to an unknown weakness. Upgrading to version 1.6.5 is able to address this issue. The patch is identified as 694da5013dbecc8d30dd83e2a83e78faadf93771. It is recommended to upgrade the affected component. VDB-217174 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2014-125037	A vulnerability, which was classified as critical, was found in License to Kill. This affects an unknown part of the file models/injury.rb. The manipulation of the argument name leads to sql injection. The patch is named cd11cf174f361c98e9b1b4c281aa7b77f46b5078. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217191.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2014-125038	A vulnerability has been found in IS_Projecto2 and classified as critical. This vulnerability affects unknown code of the file Cnn-EJB/ejbModule/ejbs/NewsBean.java. The manipulation of the argument date leads to sql injection. The name of the patch is aa128b2c9c9fdcbbf5ecd82c1e92103573017fe0. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217192.	5.5	More Details
CVE-2021-4295	A vulnerability classified as problematic was found in ONC code-validator-api up to 1.0.30. This vulnerability affects the function vocabularyValidationConfigurations of the file src/main/java/org/sitenv/vocabularies/configuration/CodeValidatorApiConfiguration.java of the component XML Handler. The manipulation leads to xml external entity reference. Upgrading to version 1.0.31 is able to address this issue. The name of the patch is fbd8ea121755a2d3d116b13f235bc8b61d8449af. It is recommended to upgrade the affected component. VDB-217018 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2016-15007	A vulnerability was found in Centralized-Salesforce-Dev-Framework. It has been declared as problematic. Affected by this vulnerability is the function SObjectService of the file src/classes/SObjectService.cls of the component SOQL Handler. The manipulation of the argument orderDirection leads to injection. The patch is named db03ac5b8a9d830095991b529c067a030a0ccf7b. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217195.	5.5	More Details
CVE-2022-4663	The Members Import plugin for WordPress is vulnerable to Self Cross-Site Scripting via the user_login parameter in an imported CSV file in versions up to, and including, 1.4.2 due to insufficient input sanitization and output escaping. This makes it possible for attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a site's administrator into uploading a CSV file with the malicious payload.	5.5	More Details
CVE-2017-20157	A vulnerability was found in Ariadne Component Library up to 2.x. It has been classified as critical. Affected is an unknown function of the file src/url/Url.php. The manipulation leads to server-side request forgery. Upgrading to version 3.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-217140.	5.5	More Details
CVE-2017-20156	A vulnerability was found in Exciting Printer and classified as critical. This issue affects some unknown processing of the file lib/printer/jobs/prepare_page.rb of the component Argument Handler. The manipulation of the argument URL leads to command injection. The patch is named 5f8c715d6e2cc000f621a6833f0a86a673462136. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217139.	5.5	More Details
CVE-2022-4362	The Popup Maker WordPress plugin before 1.16.9 does not validate and escape one of its shortcode attributes, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34323	Multiple XSS issues were discovered in Sage XRT Business Exchange 12.4.302 that allow an attacker to execute JavaScript code in the context of other users' browsers. The attacker needs to be authenticated to reach the vulnerable features. An issue is present in the Filters and Display model features (OnlineBanking > Web Monitoring > Settings > Filters / Display models). The name of a filter or a display model is interpreted as HTML and can thus embed JavaScript code, which is executed when displayed. This is a stored XSS. Another issue is present in the Notification feature (OnlineBanking > Configuration > Notifications and alerts > Alerts *). The name of an alert is interpreted as HTML, and can thus embed JavaScript code, which is executed when displayed. This is a stored XSS. (Also, an issue is present in the File download feature, accessible via /OnlineBanking/cgi/isapi.dll/DOWNLOADFRS. When requesting to show the list of downloadable files, the contents of three form fields are embedded in the JavaScript code without prior sanitization. This is essentially a self-XSS.)	5.4	More Details
CVE-2022-4381	The Popup Maker WordPress plugin before 1.16.9 does not validate and escape one of its shortcode attributes, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2022-4114	The Superio WordPress theme does not sanitise and escape some parameters, which could allow users with a role as low as a subscriber to perform Cross-Site Scripting attacks.	5.4	More Details
CVE-2022-4864	Argument Injection in GitHub repository froxlor/froxlor prior to 2.0.0-beta1.	5.4	More Details
CVE-2022-42471	An improper neutralization of CRLF sequences in HTTP headers ('HTTP Response Splitting') vulnerability [CWE-113] In FortiWeb version 7.0.0 through 7.0.2, FortiWeb version 6.4.0 through 6.4.2, FortiWeb version 6.3.6 through 6.3.20 may allow an authenticated and remote attacker to inject arbitrary headers.	5.4	More Details
CVE-2021-21200	Out of bounds read in WebUI Settings in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chrome security severity: Low)	5.4	More Details
CVE-2022-42710	Nice (formerly Nortek) Linear eMerge E3-Series 0.32-08f, 0.32-07p, 0.32-07e, 0.32-09c, 0.32-09b, 0.32-09a, and 0.32-08e devices are vulnerable to Stored Cross-Site Scripting (XSS).	5.4	More Details
CVE-2022-4840	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.9.1.	5.4	More Details
CVE-2022-4841	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.9.1.	5.4	More Details
CVE-2022-4802	Authorization Bypass Through User-Controlled Key in GitHub repository usememos/memos prior to 0.9.1.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4839	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.9.1.	5.4	More Details
CVE-2022-45213	perfSONAR before 4.4.6 inadvertently supports the parse option for a file:// URL.	5.3	More Details
CVE-2022-4057	The Autoptimize WordPress plugin before 3.1.0 uses an easily guessable path to store plugin's exported settings and logs.	5.3	More Details
CVE-2022-4851	Improper Handling of Values in GitHub repository usememos/memos prior to 0.9.1.	5.3	More Details
CVE-2022-45027	perfSONAR before 4.4.6, when performing participant discovery, incorrectly uses an HTTP request header value to determine a local address.	5.3	More Details
CVE-2022-4417	The WP Cerber Security, Anti-spam & Malware Scan WordPress plugin before 9.3.3 does not properly block access to the REST API users endpoint when the blog is in a subdirectory, which could allow attackers to bypass the restriction in place and list users	5.3	More Details
CVE-2022-4340	The BookingPress WordPress plugin before 1.0.31 suffers from an Insecure Direct Object Reference (IDOR) vulnerability in it's thank you page, allowing any visitor to display information about any booking, including full name, date, time and service booked, by manipulating the appointment_id query parameter.	5.3	More Details
CVE-2022-4806	Authorization Bypass Through User-Controlled Key in GitHub repository usememos/memos prior to 0.9.1.	5.3	More Details
CVE-2022-4804	Improper Authorization in GitHub repository usememos/memos prior to 0.9.1.	5.3	More Details
CVE-2022-4801	Insufficient Granularity of Access Control in GitHub repository usememos/memos prior to 0.9.1.	5.3	More Details
CVE-2022-4798	Authorization Bypass Through User-Controlled Key in GitHub repository usememos/memos prior to 0.9.1.	5.3	More Details
CVE-2022-42256	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer (nvidia.ko), where an integer overflow in index validation may lead to denial of service, information disclosure, or data tampering.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42255	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer (nvidia.ko), where an out-of-bounds array access may lead to denial of service, information disclosure, or data tampering.	5.3	More Details
CVE-2020-36563	XML Digital Signatures generated and validated using this package use SHA-1, which may allow an attacker to craft inputs which cause hash collisions depending on their control over the input.	5.3	More Details
CVE-2023-0029	A vulnerability was found in Multilaser RE708 RE1200R4GC-2T2R-V3_v3411b_MUL029B. It has been rated as problematic. This issue affects some unknown processing of the component Telnet Service. The manipulation leads to denial of service. The attack may be initiated remotely. The identifier VDB-217169 was assigned to this vulnerability.	5.3	More Details
CVE-2022-34684	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer (nvidia.ko), where an off-by-one error may lead to data tampering or information disclosure.	5.3	More Details
CVE-2022-42254	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer (nvidia.ko), where an out-of-bounds array access may lead to denial of service, data tampering, or information disclosure.	5.3	More Details
CVE-2013-10007	A vulnerability classified as problematic has been found in ethitter WP-Print-Friendly up to 0.5.2. This affects an unknown part of the file wp-print-friendly.php. The manipulation leads to information disclosure. It is possible to initiate the attack remotely. Upgrading to version 0.5.3 is able to address this issue. The identifier of the patch is 437787292670c20b4abe20160ebbe8428187f2b4. It is recommended to upgrade the affected component. The identifier VDB-217269 was assigned to this vulnerability.	5.3	More Details
CVE-2022-42257	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer (nvidia.ko), where an integer overflow may lead to information disclosure, data tampering or denial of service.	5.3	More Details
CVE-2022-42258	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer (nvidia.ko), where an integer overflow may lead to denial of service, data tampering, or information disclosure.	5.3	More Details
CVE-2022-42265	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer (nvidia.ko), where an integer overflow may lead to information disclosure or data tampering.	5.3	More Details
CVE-2022-4256	The All-in-One Addons for Elementor WordPress plugin before 2.4.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-4260	The WP-Ban WordPress plugin before 1.69.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4198	The WP Social Sharing WordPress plugin through 2.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2022-4200	The Login with Cognito WordPress plugin through 1.4.8 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2022-4861	Incorrect implementation in authentication protocol in M-Files Client before 22.5.11356.0 allows high privileged user to get other users tokens to another resource.	4.8	More Details
CVE-2022-3936	The Team Members WordPress plugin before 5.2.1 does not sanitize and escapes some of its settings, which could allow high-privilege users such as editors to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example, in a multisite setup).	4.8	More Details
CVE-2022-40711	PrimeKey EJBCA 7.9.0.2 Community allows stored XSS in the End Entity section. A user with the RA Administrator role can inject an XSS payload to target higher-privilege users.	4.8	More Details
CVE-2022-4119	The Image Optimizer, Resizer and CDN WordPress plugin before 6.8.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2022-4142	The WordPress Filter Gallery Plugin WordPress plugin before 0.1.6 does not properly escape the filters passed in the ufg_gallery_filters ajax action before outputting them on the page, allowing a high privileged user such as an administrator to inject HTML or javascript to the plugin settings page, even when the unfiltered_html capability is disabled.	4.8	More Details
CVE-2022-3922	The Broken Link Checker WordPress plugin before 1.11.20 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-4871	A vulnerability classified as problematic was found in ummmmm nflpick-em.com up to 2.2.x. This vulnerability affects the function _Load_Users of the file html/includes/runtime/admin/JSON/LoadUsers.php. The manipulation of the argument sort leads to sql injection. The attack can be initiated remotely. The patch is identified as dd77a35942f527ea0beef5e0ec62b92e8b93211e. It is recommended to apply a patch to fix this issue. VDB-217270 is the identifier assigned to this vulnerability. NOTE: JSON entrypoint is only accessible via an admin account	4.7	More Details
CVE-2015-10011	A vulnerability classified as problematic has been found in OpenDNS OpenResolve. This affects an unknown part of the file resolverapi/endpoints.py. The manipulation leads to improper output neutralization for logs. The identifier of the patch is 9eba6ba5abd89d0e36a008921eb307fcef8c5311. It is recommended to apply a patch to fix this issue. The identifier VDB-217197 was assigned to this vulnerability.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-20161	A vulnerability classified as problematic has been found in rofl0r MacGeiger. Affected is the function dump_wlan_at of the file macgeiger.c of the component ESSID Handler. The manipulation leads to injection. Access to the local network is required for this attack to succeed. The complexity of an attack is rather high. The exploitability is told to be difficult. The name of the patch is 57f1dd50a4821b8c8e676e8020006ae4bfd3c9cb. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217188.	4.6	More Details
CVE-2022-4780	ISOS firmwares from versions 1.81 to 2.00 contain hardcoded credentials from embedded StreamX installer that integrators are not forced to change.	4.5	More Details
CVE-2022-34673	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer (nvidia.ko), where an out-of-bounds array access may lead to denial of service, information disclosure, or data tampering.	4.4	More Details
CVE-2022-42259	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer (nvidia.ko), where an integer overflow may lead to denial of service.	4.4	More Details
CVE-2022-32639	In watchdog, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494487; Issue ID: ALPS07494487.	4.4	More Details
CVE-2022-4858	Insertion of Sensitive Information into Log Files in M-Files Server before 22.10.11846.0 could allow to obtain sensitive tokens from logs, if specific configurations were set.	4.4	More Details
CVE-2021-4299	A vulnerability classified as problematic was found in cronvel string-kit up to 0.12.7. This vulnerability affects the function naturalSort of the file lib/naturalSort.js. The manipulation leads to inefficient regular expression complexity. The attack can be initiated remotely. Upgrading to version 0.12.8 is able to address this issue. The name of the patch is 9cac4c298ee92c1695b0695951f1488884a7ca73. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-217180.	4.3	More Details
CVE-2022-4025	Inappropriate implementation in Paint in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to leak cross-origin data outside an iframe via a crafted HTML page. (Chrome security severity: Low)	4.3	More Details
CVE-2018-25053	A vulnerability was found in moappi Json2html up to 1.1.x and classified as problematic. This issue affects some unknown processing of the file json2html.js. The manipulation leads to cross site scripting. The attack may be initiated remotely. Upgrading to version 1.2.0 is able to address this issue. The name of the patch is 2d3d24d971b19a8ed1fb823596300b9835d55801. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216959.	4.3	More Details
CVE-2022-4813	Insufficient Granularity of Access Control in GitHub repository usememos/memos prior to 0.9.1.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4810	Improper Access Control in GitHub repository usememos/memos prior to 0.9.1.	4.3	More Details
CVE-2022-4868	Improper Authorization in GitHub repository froxlor/froxlor prior to 2.0.0-beta1.	4.3	More Details
CVE-2018-25061	A vulnerability was found in rgb2hex up to 0.1.5. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to inefficient regular expression complexity. The attack may be initiated remotely. Upgrading to version 0.1.6 is able to address this issue. The patch is named 9e0c38594432edfa64136fdf7bb651835e17c34f. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-217151.	4.3	More Details
CVE-2014-125028	A vulnerability was found in valtech IDP Test Client and classified as problematic. Affected by this issue is some unknown functionality of the file python-flask/main.py. The manipulation leads to cross-site request forgery. The attack may be launched remotely. The name of the patch is f1e7b3d431c8681ec46445557125890c14fa295f. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217148.	4.3	More Details
CVE-2022-4805	Incorrect Use of Privileged APIs in GitHub repository usememos/memos prior to 0.9.1.	4.3	More Details
CVE-2022-4867	Cross-Site Request Forgery (CSRF) in GitHub repository froxlor/froxlor prior to 2.0.0-beta1.	4.3	More Details
CVE-2022-4797	Improper Restriction of Excessive Authentication Attempts in GitHub repository usememos/memos prior to 0.9.1.	4.3	More Details
CVE-2022-3994	The Authenticator WordPress plugin before 1.3.1 does not prevent subscribers from updating a site's feed access token, which may deny other users access to the functionality in certain configurations.	4.3	More Details
CVE-2022-4814	Improper Access Control in GitHub repository usememos/memos prior to 0.9.1.	4.3	More Details
CVE-2022-4807	Improper Access Control in GitHub repository usememos/memos prior to 0.9.1.	4.3	More Details
CVE-2022-4845	Cross-Site Request Forgery (CSRF) in GitHub repository usememos/memos prior to 0.9.1.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23506	Spinnaker is an open source, multi-cloud continuous delivery platform for releasing software changes, and Spinnaker's Rosco microservice produces machine images. Rosco prior to versions 1.29.2, 1.28.4, and 1.27.3 does not property mask secrets generated via packer builds. This can lead to exposure of sensitive AWS credentials in packer log files. Versions 1.29.2, 1.28.4, and 1.27.3 of Rosco contain fixes for this issue. A workaround is available. It's recommended to use short lived credentials via role assumption and IAM profiles. Additionally, credentials can be set in `/home/spinnaker/.aws/credentials` and `/home/spinnaker/.aws/config` as a volume mount for Rosco pods vs. setting credentials in roscos bake config properties. Last even with those it's recommend to use IAM Roles vs. long lived credentials. This drastically mitigates the risk of credentials exposure. If users have used static credentials, it's recommended to purge any bake logs for AWS, evaluate whether AWS_ACCESS_KEY, SECRET_KEY and/or other sensitive data has been introduced in log files and bake job logs. Then, rotate these credentials and evaluate potential improper use of those credentials.	4.3	More Details
CVE-2022-46174	efs-utils is a set of Utilities for Amazon Elastic File System (EFS). A potential race condition issue exists within the Amazon EFS mount helper in efs-utils versions v1.34.3 and below. When using TLS to mount file systems, the mount helper allocates a local port for stunnel to receive NFS connections prior to applying the TLS tunnel. In affected versions, concurrent mount operations can allocate the same local port, leading to either failed mount operations or an inappropriate mapping from an EFS customer’s local mount points to that customer’s EFS file systems. This issue is patched in version v1.34.4. There is no recommended work around. We recommend affected users update the installed version of efs-utils to v1.34.4 or later.	4.2	More Details
CVE-2018-25058	A vulnerability classified as problematic has been found in Twitter-Post-Fetcher up to 17.x. This affects an unknown part of the file js/twitterFetcher.js of the component Link Target Handler. The manipulation leads to use of web link to untrusted target with window.opener access. It is possible to initiate the attack remotely. Upgrading to version 18.0.0 is able to address this issue. The name of the patch is 7d281c6fb5acbc29a2cad295262c1f0c19ca56f3. It is recommended to upgrade the affected component. The identifier VDB-217017 was assigned to this vulnerability.	4.2	More Details
CVE-2022-32645	In vow, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494477; Issue ID: ALPS07494477.	4.1	More Details
CVE-2016-15006	A vulnerability, which was classified as problematic, has been found in enigmaX up to 2.2. This issue affects the function getSeed of the file main.c of the component Scrambling Table Handler. The manipulation leads to predictable seed in pseudo-random number generator (prng). The attack may be initiated remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. Upgrading to version 2.3 is able to address this issue. The identifier of the patch is 922bf90ca14a681629ba0b807a997a81d70225b5. It is recommended to upgrade the affected component. The identifier VDB-217181 was assigned to this vulnerability.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-25060	A vulnerability was found in Macaron csrf and classified as problematic. Affected by this issue is some unknown functionality of the file csrf.go. The manipulation of the argument Generate leads to sensitive cookie without secure attribute. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The patch is identified as dadd1711a617000b70e5e408a76531b73187031c. It is recommended to apply a patch to fix this issue. VDB-217058 is the identifier assigned to this vulnerability.	3.7	More Details
CVE-2020-36638	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in Chris92de AdminServ. It has been rated as problematic. This issue affects some unknown processing of the file resources/core/adminserv.php. The manipulation of the argument error leads to cross site scripting. The attack may be initiated remotely. The patch is named 9a45087814295de6fb3a3fe38f96293665234da1. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217043. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	3.5	More Details
CVE-2015-10012	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in sumocoders FrameworkUserBundle up to 1.3.x. It has been rated as problematic. Affected by this issue is some unknown functionality of the file Resources/views/Security/login.html.twig. The manipulation leads to information exposure through error message. Upgrading to version 1.4.0 is able to address this issue. The name of the patch is abe4993390ba9bd7821ab12678270556645f94c8. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-217268. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	3.5	More Details
CVE-2014-125027	A vulnerability has been found in Yuna Scatari TBDev up to 2.1.17 and classified as problematic. Affected by this vulnerability is the function get_user_icons of the file usersearch.php. The manipulation of the argument n/r/r2/em/ip/co/ma/d/d2/ul/ul2/ls/ls2/dl/dl2 leads to cross site scripting. The attack can be launched remotely. Upgrading to version 2.1.18 is able to address this issue. The patch is named 0ba3fd4be29dd48fa4455c236a9403b3149a4fd4. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-217147.	3.5	More Details
CVE-2017-20159	A vulnerability was found in rf Keynote up to 0.x on Rails. It has been rated as problematic. Affected by this issue is some unknown functionality of the file lib/keynote/rumble.rb. The manipulation of the argument value leads to cross site scripting. The attack may be launched remotely. Upgrading to version 1.0.0 is able to address this issue. The patch is identified as 05be4356b0a6ca7de48da926a9b997beb5ffeb4a. It is recommended to upgrade the affected component. VDB-217142 is the identifier assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-20158	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in vova07 Yii2 FileAPI Widget up to 0.1.8. It has been declared as problematic. Affected by this vulnerability is the function run of the file actions/UploadAction.php. The manipulation of the argument file leads to cross site scripting. The attack can be launched remotely. Upgrading to version 0.1.9 is able to address this issue. The identifier of the patch is c00d1e4fc912257fca1fce66d7a163bdbb4c8222. It is recommended to upgrade the affected component. The identifier VDB-217141 was assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	3.5	More Details
CVE-2014-125035	A vulnerability classified as problematic was found in Jobs-Plugin. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. The attack can be launched remotely. The identifier of the patch is b8a56718b1d42834c6ec51d9c489c5dc20471d7b. It is recommended to apply a patch to fix this issue. The identifier VDB-217189 was assigned to this vulnerability.	3.5	More Details
CVE-2012-10003	A vulnerability, which was classified as problematic, has been found in ahmyi RivetTracker. This issue affects some unknown processing. The manipulation of the argument $_SERVER['PHP_SELF'] leads to cross site scripting. The attack may be initiated remotely. The patch is named f053c5cc2bc44269b0496b5f275e349928a92ef9. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217271.	3.5	More Details
CVE-2018-25052	A vulnerability has been found in Catalyst-Plugin-Session up to 0.40 and classified as problematic. This vulnerability affects the function _load_sessionid of the file lib/Catalyst/Plugin/Session.pm of the component Session ID Handler. The manipulation of the argument sid leads to cross site scripting. The attack can be initiated remotely. Upgrading to version 0.41 is able to address this issue. The name of the patch is 88d1b599e1163761c9bd53bec53ba078f13e09d4. It is recommended to upgrade the affected component. VDB-216958 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2018-25062	A vulnerability classified as problematic has been found in flar2 ElementalX up to 6.x on Nexus 9. Affected is the function xfrm_dump_policy_done of the file net/xfrm/xfrm_user.c of the component ipsec. The manipulation leads to denial of service. Upgrading to version 7.00 is able to address this issue. The name of the patch is 1df72c9f0f61304437f4f1037df03b5fb36d5a79. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-217152.	3.5	More Details
CVE-2022-4859	A vulnerability, which was classified as problematic, has been found in Joget up to 7.0.33. This issue affects the function submitForm of the file wflow-core/src/main/java/org/joget/plugin/enterprise/UserProfileMenu.java of the component User Profile Menu. The manipulation of the argument firstName/lastName leads to cross site scripting. The attack may be initiated remotely. Upgrading to version 7.0.34 is able to address this issue. The patch is named 9a77f508a2bf8cf661d588f37a4cc29ecaea4fc8. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-217055.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4820	A vulnerability classified as problematic has been found in FlatPress. This affects an unknown part of the file admin/panels/entry/admin.entry.list.php of the component Admin Area. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The name of the patch is 229752b51025e678370298284d42f8ebb231f67f. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-216999.	3.5	More Details
CVE-2021-4296	A vulnerability, which was classified as problematic, has been found in w3c Unicorn. This issue affects the function ValidatorNuMessage of the file src/org/w3c/unicorn/response/impl/ValidatorNuMessage.java. The manipulation of the argument message leads to cross site scripting. The attack may be initiated remotely. The name of the patch is 51f75c31f7fc33859a9a571311c67ae4e95d9c68. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217019.	3.5	More Details
CVE-2018-25056	A vulnerability, which was classified as problematic, was found in yolapi. Affected is the function render_description of the file yolapi/pypi/metadata.py. The manipulation of the argument text leads to cross site scripting. It is possible to launch the attack remotely. The name of the patch is a0fe129055a99f429133a5c40cb13b44611ff796. It is recommended to apply a patch to fix this issue. VDB-216966 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2018-25055	A vulnerability was found in FarCry Solr Pro Plugin up to 1.5.x. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file packages/forms/solrProSearch.cfc of the component Search Handler. The manipulation of the argument suggestion leads to cross site scripting. The attack can be launched remotely. Upgrading to version 1.6.0 is able to address this issue. The name of the patch is b8f3d61511c9b02b781ec442bfb803cbff8e08d5. It is recommended to upgrade the affected component. The identifier VDB-216961 was assigned to this vulnerability.	3.5	More Details
CVE-2018-25054	A vulnerability was found in shred cilla. It has been classified as problematic. Affected is an unknown function of the file cilla-xample/src/main/webapp/WEB-INF/jsp/view/search.jsp of the component Search Handler. The manipulation of the argument details leads to cross site scripting. It is possible to launch the attack remotely. The name of the patch is d345e6bc7798bd717a583ec7f545ca387819d5c7. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-216960.	3.5	More Details
CVE-2012-10002	A vulnerability was found in ahmyi RivetTracker. It has been declared as problematic. Affected by this vulnerability is the function changeColor of the file css.php. The manipulation of the argument set_css leads to cross site scripting. The attack can be launched remotely. The patch is named 45a0f33876d58cb7e4a0f17da149e58fc893b858. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217267.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-20155	A vulnerability was found in Sterc Google Analytics Dashboard for MODX up to 1.0.5. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file core/components/analyticsdashboardwidget/elements/tpl/widget.analytics.tpl of the component Internal Search. The manipulation leads to cross site scripting. The attack can be launched remotely. Upgrading to version 1.0.6 is able to address this issue. The identifier of the patch is 855d9560d3782c105568eedf9b22a769fbf29cc0. It is recommended to upgrade the affected component. The identifier VDB-217069 was assigned to this vulnerability.	3.5	More Details
CVE-2017-20154	A vulnerability was found in ghostlander Phoenixcoin. It has been classified as problematic. Affected is the function CTxMemPool::accept of the file src/main.cpp. The manipulation leads to denial of service. Upgrading to version 0.6.6.1-pxc is able to address this issue. The name of the patch is 987dd68f71a7d8276cef3b6c3d578fd4845b5699. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-217068.	3.5	More Details
CVE-2020-36637	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in Chris92de AdminServ. It has been declared as problematic. This vulnerability affects unknown code of the file resources/core/adminserv.php. The manipulation of the argument text leads to cross site scripting. The attack can be initiated remotely. The patch is identified as 3ed17dab3b4d6e8bf1c82ddfbf882314365e9cd7. It is recommended to apply a patch to fix this issue. VDB-217042 is the identifier assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	3.5	More Details
CVE-2014-125034	A vulnerability has been found in stiiv contact_app and classified as problematic. Affected by this vulnerability is the function render of the file libs/View.php. The manipulation of the argument var leads to cross site scripting. The attack can be launched remotely. The patch is named 67bec33f559da9d41a1b45eb9e992bd8683a7f8c. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217183.	3.5	More Details
CVE-2014-125033	A vulnerability was found in rails-cv-app. It has been rated as problematic. Affected by this issue is some unknown functionality of the file app/controllers/uploaded_files_controller.rb. The manipulation with the input ../../../etc/passwd leads to path traversal: '../filedir'. The exploit has been disclosed to the public and may be used. The patch is identified as 0d20362af0a5f8a126f67c77833868908484a863. It is recommended to apply a patch to fix this issue. VDB-217178 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2018-25050	A vulnerability, which was classified as problematic, has been found in Harvest Chosen up to 1.8.6. Affected by this issue is the function AbstractChosen of the file coffee/lib/abstract-chosen.coffee. The manipulation of the argument group_label leads to cross site scripting. The attack may be launched remotely. Upgrading to version 1.8.7 is able to address this issue. The name of the patch is 77fd031d541e77510268d1041ed37798fdd1017e. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-216956.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-25059	A vulnerability was found in pastebinit up to 0.2.2 and classified as problematic. Affected by this issue is the function pasteHandler of the file server.go. The manipulation of the argument r.URL.Path leads to path traversal. Upgrading to version 0.2.3 is able to address this issue. The name of the patch is 1af2facb6d95976c532b7f8f82747d454a092272. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-217040.	3.5	More Details
CVE-2014-125031	A vulnerability was found in kirill2485 TekNet. It has been classified as problematic. Affected is an unknown function of the file pages/loggedin.php. The manipulation of the argument statusentery leads to cross site scripting. It is possible to launch the attack remotely. The name of the patch is 1c575340539f983333aa43fc58ecd76eb53e1816. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217176.	3.5	More Details
CVE-2021-4293	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as problematic has been found in gnuboard youngcart5 up to 5.4.5.1. Affected is an unknown function of the file adm/menu_list_update.php. The manipulation of the argument me_link leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 5.4.5.2 is able to address this issue. The name of the patch is 70daa537adfa47b87af12d85f1e698fff01785ff. It is recommended to upgrade the affected component. VDB-216954 is the identifier assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	3.5	More Details
CVE-2018-25063	A vulnerability classified as problematic was found in Zenoss Dashboard up to 1.3.4. Affected by this vulnerability is an unknown functionality of the file ZenPacks/zenoss/Dashboard/browser/resources/js/defaultportlets.js. The manipulation of the argument HTMLString leads to cross site scripting. The attack can be launched remotely. Upgrading to version 1.3.5 is able to address this issue. The identifier of the patch is f462285a0a2d7e1a9255b0820240b94a43b00a44. It is recommended to upgrade the affected component. The identifier VDB-217153 was assigned to this vulnerability.	3.5	More Details
CVE-2015-10006	A vulnerability, which was classified as problematic, has been found in admont28 Ingnovarq. Affected by this issue is some unknown functionality of the file app/controller/insertarSliderAjax.php. The manipulation of the argument imagetitle leads to cross site scripting. The attack may be launched remotely. The name of the patch is 9d18a39944d79dfedacd754a742df38f99d3c0e2. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217172.	3.5	More Details
CVE-2015-10007	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in 82Flex WEIPDCRM and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. The attack may be launched remotely. The name of the patch is 43bad79392332fa39e31b95268e76fbda9fec3a4. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217184. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47952	lxc-user-nic in lxc through 5.0.1 is installed setuid root, and may allow local users to infer whether any file exists, even within a protected directory tree, because "Failed to open" often indicates that a file does not exist, whereas "does not refer to a network namespace path" often indicates that a file exists. NOTE: this is different from CVE-2018-6556 because the CVE-2018-6556 fix design was based on the premise that "we will report back to the user that the open() failed but the user has no way of knowing why it failed"; however, in many realistic cases, there are no plausible reasons for failing except that the file does not exist.	3.3	More Details
CVE-2010-10002	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as problematic has been found in SimpleSAMLphp simplesamlphp-module-openid. Affected is an unknown function of the file templates/consumer.php of the component OpenID Handler. The manipulation of the argument AuthState leads to cross site scripting. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. Upgrading to version 1.0 is able to address this issue. The patch is identified as d652d41ccaf8c45d5707e741c0c5d82a2365a9a3. It is recommended to upgrade the affected component. VDB-217170 is the identifier assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	3.1	More Details
CVE-2015-10010	A vulnerability was found in OpenDNS OpenResolve. It has been rated as problematic. Affected by this issue is the function get of the file resolverapi/endpoints.py of the component API. The manipulation leads to cross site scripting. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The name of the patch is c680170d5583cd9342fe1af43001fe8b2b8004dd. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217196.	3.1	More Details
CVE-2022-4817	A vulnerability was found in centic9 jgit-cookbook. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to insecure temporary file. The attack can be initiated remotely. The name of the patch is b8cb29b43dc704708d598c60ac1881db7cf8e9c3. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-216988.	3.1	More Details
CVE-2022-4823	A vulnerability, which was classified as problematic, was found in InSTEDD Nuntium. Affected is an unknown function of the file app/controllers/geopoll_controller.rb. The manipulation of the argument signature leads to observable timing discrepancy. It is possible to launch the attack remotely. The name of the patch is 77236f7fd71a0e2eefeea07f9866b069d612cf0d. It is recommended to apply a patch to fix this issue. VDB-217002 is the identifier assigned to this vulnerability.	3.1	More Details
CVE-2017-20152	A vulnerability, which was classified as problematic, was found in aerouk imageserve. Affected is an unknown function of the file public/viewer.php of the component File Handler. The manipulation of the argument filelocation leads to path traversal. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The name of the patch is bd23c784f0e5cb12f66d15c100248449f87d72e2. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217056.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4109	The Wholesale Market for WooCommerce WordPress plugin before 2.0.0 does not validate user input against path traversal attacks, allowing high privilege users such as admin to download arbitrary logs from the server even when they should not be able to (for example in multisite)	2.7	More Details
CVE-2013-10006	A vulnerability classified as problematic was found in Ziftr primecoin up to 0.8.4rc1. Affected by this vulnerability is the function HTTPAuthorized of the file src/bitcoinrpc.cpp. The manipulation of the argument strUserPass/strRPCUserColonPass leads to observable timing discrepancy. The complexity of an attack is rather high. The exploitation appears to be difficult. Upgrading to version 0.8.4rc2 is able to address this issue. The patch is named cdb3441b5cd2c1bae49fae671dc4a496f7c96322. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-217171.	2.6	More Details
CVE-2014-125036	A vulnerability, which was classified as problematic, has been found in drybjed ansible-ntp. Affected by this issue is some unknown functionality of the file meta/main.yml. The manipulation leads to insufficient control of network message volume. The attack can only be done within the local network. The complexity of an attack is rather high. The exploitation is known to be difficult. The patch is identified as ed4ca2cf012677973c220cdba36b5c60bfa0260b. It is recommended to apply a patch to fix this issue. VDB-217190 is the identifier assigned to this vulnerability.	2.6	More Details
CVE-2017-20153	A vulnerability has been found in aerouk imageserve and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument REQUEST_URI leads to cross site scripting. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The identifier of the patch is 2ac3cd4f90b4df66874fab171376ca26868604c4. It is recommended to apply a patch to fix this issue. The identifier VDB-217057 was assigned to this vulnerability.	2.6	More Details
CVE-2021-4294	A vulnerability was found in OpenShift OSIN. It has been classified as problematic. This affects the function ClientSecretMatches/CheckClientSecret. The manipulation of the argument secret leads to observable timing discrepancy. The name of the patch is 8612686d6dda34ae9ef6b5a974e4b7accb4fea29. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-216987.	2.6	More Details
CVE-2022-4773	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as problematic was found in cloudsync. Affected by this vulnerability is the function getItem of the file src/main/java/cloudsync/connector/LocalFilesystemConnector.java. The manipulation leads to path traversal. It is possible to launch the attack on the local host. The name of the patch is 3ad796833398af257c28e0ebeade68518e0e612a. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-216919. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-25092	A vulnerability classified as problematic was found in Nakiami Mellivora up to 2.1.x. Affected by this vulnerability is the function print_user_ip_log of the file include/layout/user.inc.php of the component Admin Panel. The manipulation of the argument $entry['ip'] leads to cross site scripting. The attack can be launched remotely. Upgrading to version 2.2.0 is able to address this issue. The name of the patch is e0b6965f8dde608a3d2621617c05695eb406cbb9. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216955.	2.4	More Details
CVE-2019-25093	A vulnerability, which was classified as problematic, was found in dragonexpert Recent Threads on Index. Affected is the function recentthread_list_threads of the file inc/plugins/recentthreads/hooks.php of the component Setting Handler. The manipulation of the argument recentthread_forumskip leads to cross site scripting. It is possible to launch the attack remotely. The patch is identified as 051465d807a8fcc6a8b0f4bcbb19299672399f48. It is recommended to apply a patch to fix this issue. VDB-217182 is the identifier assigned to this vulnerability.	2.4	More Details
CVE-2018-25051	A vulnerability, which was classified as problematic, was found in JmPotato Pomash. This affects an unknown part of the file Pomash/theme/clean/templates/editor.html. The manipulation of the argument article.title/content.title/article.tag leads to cross site scripting. It is possible to initiate the attack remotely. The name of the patch is be1914ef0a6808e00f51618b2de92496a3604415. It is recommended to apply a patch to fix this issue. The identifier VDB-216957 was assigned to this vulnerability.	2.4	More Details
CVE-2022-4821	A vulnerability classified as problematic was found in FlatPress. This vulnerability affects the function onupload of the file admin/panels/uploader/admin.uploader.php of the component XML File Handler/MD File Handler. The manipulation leads to cross site scripting. The attack can be initiated remotely. The name of the patch is 3cc223dec5260e533a84b5cf5780d3a4fbf21241. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217000.	2.4	More Details
CVE-2022-4819	A vulnerability was found in HotCRP. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. The attack may be launched remotely. The name of the patch is d4ffdb0ef806453c54ddca7fdda3e5c60356285c. It is recommended to apply a patch to fix this issue. VDB-216998 is the identifier assigned to this vulnerability.	2.4	More Details
CVE-2022-4822	A vulnerability, which was classified as problematic, has been found in FlatPress. This issue affects some unknown processing of the file setup/lib/main.lib.php of the component Setup. The manipulation leads to cross site scripting. The attack may be initiated remotely. The name of the patch is 5f23b4c2eac294cc0ba5e541f83a6f8a26f9fed1. It is recommended to apply a patch to fix this issue. The identifier VDB-217001 was assigned to this vulnerability.	2.4	More Details
CVE-2020-12573	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-43811	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43817	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43815	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43814	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43813	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43812	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43810	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43819	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43809	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43808	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43807	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43806	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2020-12568	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-43805	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43818	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43820	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2020-12574	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-43821	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43822	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43823	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43824	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43825	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43826	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43827	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43828	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2020-12569	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12570	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12571	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-43829	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2020-12572	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-43830	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43816	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2020-2059	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12567	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12520	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12540	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12539	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12538	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12537	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12536	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12535	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12534	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12533	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12532	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12531	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12515	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12542	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2019-17443	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2019-17442	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2019-17441	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2019-17439	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2019-17438	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2019-11824	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3905	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2017-12073	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-39159	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-0039	Rejected reason: Duplicate. Please use CVE-2022-4060 instead.	N/A	More Details
CVE-2020-12541	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12543	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12566	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12555	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12565	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12564	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12563	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12562	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12561	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12560	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12559	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12558	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12557	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12556	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12554	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12544	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12553	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12552	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12551	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12550	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-43803	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2020-12549	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12548	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12547	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12546	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12545	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-43804	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43794	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43802	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2021-3096	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23108	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23107	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23106	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23105	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23104	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23103	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23102	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23101	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23100	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23099	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23098	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23097	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23096	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23095	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23094	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23093	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23092	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23091	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23090	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23109	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23110	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23111	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23122	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-3093	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-3092	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-34608	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-34607	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-34603	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-27650	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-26568	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-24417	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23121	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23112	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23120	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23119	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23118	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23117	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23116	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23115	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23114	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23113	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23089	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23088	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23087	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2074	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23063	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23062	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23061	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23060	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23059	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23058	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23057	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23056	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-2073	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23065	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-2072	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-2071	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2069	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-2068	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-2067	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-2065	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-2064	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-2062	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23064	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23066	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23086	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23077	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23085	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23084	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23083	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23082	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23081	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23080	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23079	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23078	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23076	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23067	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23075	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23074	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23073	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23072	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23071	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23070	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23069	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-23068	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-3094	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-2058	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-43801	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2021-3098	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12577	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12578	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12579	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12580	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12581	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12582	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12583	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12584	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12585	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12586	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12587	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12588	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12589	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12590	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12591	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12592	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-2045	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-2046	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-2047	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-12576	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12575	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-36816	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43792	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43800	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43799	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43798	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43797	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43796	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43795	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2020-2061	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-43793	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43791	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-36827	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43790	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43789	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43788	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43787	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43786	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43785	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43784	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2022-43783	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2020-2051	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-2052	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-2053	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-2349	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-42738	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42737	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-41857	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-41856	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-41855	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-3778	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-3692	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-2530	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-2348	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-42740	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-22200	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-22199	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-22165	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-22158	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3105	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-3104	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-3103	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-3102	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-42739	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-42741	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-2054	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-46672	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-2056	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-2057	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-4659	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-4618	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-4339	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4334	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-4168	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-46673	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-46671	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-42742	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-46669	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-46668	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-46667	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-46666	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-46665	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-43944	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-43943	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-43942	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3097	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details