SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 20 September 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-2023-41892	Craft CMS is a platform for creating digital experiences. This is a high-impact, low-complexity attack vector. Users running Craft installations before 4.4.15 are encouraged to update to at least that version to mitigate the issue. This issue has been fixed in Craft CMS 4.4.15.	10.0	More Details
CVE-2023-42454	SQLpage is a SQL-only webapp builder. Someone using SQLpage versions prior to 0.11.1, whose SQLpage instance is exposed publicly, with a database connection string specified in the `sqlpage/sqlpage.json` configuration file (not in an environment variable), with the web_root is the current working directory (the default), and with their database exposed publicly, is vulnerable to an attacker retrieving database connection information from SQLPage and using it to connect to their database directly. Version 0.11.0 fixes this issue. Some workarounds are available. Using an environment variable instead of the configuration file to specify the database connection string prevents exposing it on vulnerable versions. Using a different web root (that is not a parent of the SQLPage configuration directory) fixes the issue. One should also avoid exposing one's database publicly.	10.0	More Details
CVE-2023-41084	Session management within the web application is incorrect and allows attackers to steal session cookies to perform a multitude of actions that the web app allows on the device.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4994	The Allow PHP in Posts and Pages plugin for WordPress is vulnerable to Remote Code Execution in versions up to, and including, 3.0.4 via the 'php' shortcode. This allows authenticated attackers with subscriber-level permissions or above, to execute code on the server.	9.9	More Details
CVE-2023-3935	A heap buffer overflow vulnerability in Wibu CodeMeter Runtime network service up to version 7.60b allows an unauthenticated, remote attacker to achieve RCE and gain full access of the host system.	9.8	More Details
CVE-2023-42398	An issue in zzCMS v.2023 allows a remote attacker to execute arbitrary code and obtain sensitive information via the ueditor component in controller.php.	9.8	More Details
CVE-2023-4231	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Cevik Informatics Online Payment System allows SQL Injection.This issue affects Online Payment System: before 4.09.	9.8	More Details
CVE-2023-4831	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ncode Ncep allows SQL Injection.This issue affects Ncep: before 20230914 .	9.8	More Details
CVE-2023-4661	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Saphira Saphira Connect allows SQL Injection.This issue affects Saphira Connect: before 9.	9.8	More Details
CVE-2023-4662	Execution with Unnecessary Privileges vulnerability in Saphira Saphira Connect allows Remote Code Inclusion.This issue affects Saphira Connect: before 9.	9.8	More Details
CVE-2023-4833	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Besttem Network Marketing Software allows SQL Injection.This issue affects Network Marketing Software: before 1.0.2309.6.	9.8	More Details
CVE-2023-4835	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CF Software Oil Management Software allows SQL Injection.This issue affects Oil Management Software: before 20230912 .	9.8	More Details
CVE-2023-28614	Freewill iFIS (aka SMART Trade) 20.01.01.04 allows OS Command Injection via shell metacharacters to a report page.	9.8	More Details
CVE-2023-42336	An issue in NETIS SYSTEMS WF2409Ev4 v.1.0.1.705 allows a remote attacker to execute arbitrary code and obtain sensitive information via the password parameter in the /etc/shadow.sample component.	9.8	More Details
CVE-2023-41887	OpenRefine is a powerful free, open source tool for working with messy data. Prior to version 3.7.5, a remote code execution vulnerability allows any unauthenticated user to execute code on the server. Version 3.7.5 has a patch for this issue.	9.8	More Details
CVE-2023-4673	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Sanalogy Turasistan allows SQL Injection.This issue affects Turasistan: before 20230911 .	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42359	SQL injection vulnerability in Exam Form Submission in PHP with Source Code v.1.0 allows a remote attacker to escalate privileges via the val-username parameter in /index.php.	9.8	More Details
CVE-2023-42320	Buffer Overflow vulnerability in Tenda AC10V4 v.US_AC10V4.0si_V16.03.10.13_cn_TDC01 allows a remote attacker to cause a denial of service via the mac parameter in the GetParentControlInfo function.	9.8	More Details
CVE-2023-33831	A remote command execution (RCE) vulnerability in the /api/runscript endpoint of FUXA 1.1.13 allows attackers to execute arbitrary commands via a crafted POST request.	9.8	More Details
CVE-2021-26837	SQL Injection vulnerability in SearchTextBox parameter in Fortra (Formerly HelpSystems) DeliverNow before version 1.2.18, allows attackers to execute arbitrary code, escalate privileges, and gain sensitive information.	9.8	More Details
CVE-2022-28357	NATS nats-server 2.2.0 through 2.7.4 allows directory traversal because of an unintended path to a management action from a management account.	9.8	More Details
CVE-2023-4830	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Tura Signalix allows SQL Injection.This issue affects Signalix: 7T_0228.	9.8	More Details
CVE-2023-4670	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Innosa Probbys allows SQL Injection.This issue affects Probbys: before 2.	9.8	More Details
CVE-2023-36659	An issue was discovered in OPSWAT MetaDefender KIOSK 4.6.1.9996. Long inputs were not properly processed, which allows remote attackers to cause a denial of service (loss of communication).	9.8	More Details
CVE-2023-36657	An issue was discovered in OPSWAT MetaDefender KIOSK 4.6.1.9996. Built-in features of Windows (desktop shortcuts, narrator) can be abused for privilege escalation.	9.8	More Details
CVE-2023-38204	Adobe ColdFusion versions 2018u18 (and earlier), 2021u8 (and earlier) and 2023u2 (and earlier) are affected by a Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution. Exploitation of this issue does not require user interaction.	9.8	More Details
CVE-2023-30909	A remote authentication bypass issue exists in some OneView APIs.	9.8	More Details
CVE-2023-4832	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Aceka Company Management allows SQL Injection.This issue affects Company Management: before 3072 .	9.8	More Details
CVE-2023-41011	Command Execution vulnerability in China Mobile Communications China Mobile Intelligent Home Gateway v.HG6543C4 allows a remote attacker to execute arbitrary code via the shortcut_telnet.cg component.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4669	Authentication Bypass by Assumed-Immutable Data vulnerability in Exagate SYSGuard 3001 allows Authentication Bypass.This issue affects SYSGuard 3001: before 3.2.20.0.	9.8	More Details
CVE-2023-4766	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Movus allows SQL Injection.This issue affects Movus: before 20230913.	9.8	More Details
CVE-2023-37755	i-doit pro 25 and below and I-doit open 25 and below are configured with insecure default administrator credentials, and there is no warning or prompt to ask users to change the default password and account name. Unauthenticated attackers can exploit this vulnerability to obtain Administrator privileges, resulting in them being able to perform arbitrary system operations or cause a Denial of Service (DoS).	9.8	More Details
CVE-2023-4702	Authentication Bypass Using an Alternate Path or Channel vulnerability in Yepas Digital Yepas allows Authentication Bypass.This issue affects Digital Yepas: before 1.0.1.	9.8	More Details
CVE-2023-4972	Incorrect Use of Privileged APIs vulnerability in Yepas Digital Yepas allows Collect Data as Provided by Users.This issue affects Digital Yepas: before 1.0.1.	9.8	More Details
CVE-2023-37756	I-doit pro 25 and below and I-doit open 25 and below employ weak password requirements for Administrator account creation. Attackers are able to easily guess users' passwords via a bruteforce attack.	9.8	More Details
CVE-2023-38912	SQL injection vulnerability in Super Store Finder PHP Script v.3.6 allows a remote attacker to execute arbitrary code via a crafted payload to the username parameter.	9.8	More Details
CVE-2023-39638	D-LINK DIR-859 A1 1.05 and A1 1.06B01 Beta01 was discovered to contain a command injection vulnerability via the lxmldbc_system function at /htdocs/cgibin.	9.8	More Details
CVE-2023-42405	SQL injection vulnerability in FIT2CLOUD RackShift v1.7.1 allows attackers to execute arbitrary code via the `sort` parameter to taskService.list(), bareMetalService.list(), and switchService.list().	9.8	More Details
CVE-2023-39639	LeoTheme leoblog up to v3.1.2 was discovered to contain a SQL injection vulnerability via the component LeoBlogBlog::getListBlogs.	9.8	More Details
CVE-2023-39641	Active Design psaffiliate before v1.9.8 was discovered to contain a SQL injection vulnerability via the component PsaffiliateGetaffiliatesdetailsModuleFrontController::initContent().	9.8	More Details
CVE-2023-39642	Carts Guru cartsguru up to v2.4.2 was discovered to contain a SQL injection vulnerability via the component CartsGuruCatalogModuleFrontController::display().	9.8	More Details
CVE-2023-39643	Bl Modules xmlfeeds before v3.9.8 was discovered to contain a SQL injection vulnerability via the component SearchApiXml::Xmlfeeds().	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42793	In JetBrains TeamCity before 2023.05.4 authentication bypass leading to RCE on TeamCity Server was possible	9.8	More Details
CVE-2023-36735	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	9.6	More Details
CVE-2022-47558	Devices ekorCCP and ekorRCI are vulnerable due to access to the FTP service using default credentials. Exploitation of this vulnerability can allow an attacker to modify critical files that could allow the creation of new users, delete or modify existing users, modify configuration files, install rootkits or backdoors.	9.4	More Details
CVE-2023-39916	NLnet Labs' Routinator 0.9.0 up to and including 0.12.1 contains a possible path traversal vulnerability in the optional, off-by-default keep-rrdp-responses feature that allows users to store the content of responses received for RRDP requests. The location of these stored responses is constructed from the URL of the request. Due to insufficient sanitation of the URL, it is possible for an attacker to craft a URL that results in the response being stored outside of the directory specified for it.	9.3	More Details
CVE-2022-47555	Operating system command injection in ekorCCP and ekorRCI, which could allow an authenticated attacker to execute commands, create new users with elevated privileges or set up a backdoor.	9.3	More Details
CVE-2023-41387	A SQL injection in the flutter_downloader component through 1.11.1 for iOS allows remote attackers to steal session tokens and overwrite arbitrary files inside the app's container. The internal database of the framework is exposed to the local user if an app uses UIFileSharingEnabled and LSSupportsOpeningDocumentsInPlace properties. As a result, local users can obtain the same attack primitives as remote attackers by tampering with the internal database of the framework on the device.	9.1	More Details
CVE-2023-0773	The vulnerability exists in Uniview IP Camera due to identification and authentication failure at its web-based management interface. A remote attacker could exploit this vulnerability by sending specially crafted HTTP requests to the vulnerable device. Successful exploitation of this vulnerability could allow the attacker to gain complete control of the targeted device.	9.1	More Details
CVE-2023-39612	A cross-site scripting (XSS) vulnerability in FileBrowser before v2.23.0 allows an authenticated attacker to escalate privileges to Administrator via user interaction with a crafted HTML file or URL.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-39446	Thanks to the weaknesses that the web application has at the user management level, an attacker could obtain the information from the headers that is necessary to create specially designed URLs and originate malicious actions when a legitimate user is logged into the web application.	8.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2567	A SQL Injection vulnerability has been found in Nozomi Networks Guardian and CMC, due to improper input validation in certain parameters used in the Query functionality. Authenticated users may be able to execute arbitrary SQL statements on the DBMS used by the web application.	8.8	More Details
CVE-2023-40957	A SQL injection vulnerability in Didotech srl Engineering & Lifecycle Management (aka pdm) v.14.0, v.15.0 and v.16.0 fixed in pdm-14.0.1.0.0, pdm-15.0.1.0.0, and pdm-16.0.1.0.0 allows a remote authenticated attacker to execute arbitrary code via the request parameter in models/base_client.py component.	8.8	More Details
CVE-2023-40958	A SQL injection vulnerability in Didotech srl Engineering & Lifecycle Management (aka pdm) v.14.0, v.15.0 and v.16.0 fixed in pdm-14.0.1.0.0, pdm-15.0.1.0.0, and pdm-16.0.1.0.0 allows a remote authenticated attacker to execute arbitrary code via the query parameter in models/base_client.py component.	8.8	More Details
CVE-2023-4092	SQL injection vulnerability in Arconte Áurea, in its 1.5.0.0 version. The exploitation of this vulnerability could allow an attacker to read sensitive data from the database, modify data (insert/update/delete), perform database administration operations and, in some cases, execute commands on the operating system.	8.8	More Details
CVE-2023-4664	Incorrect Default Permissions vulnerability in Saphira Saphira Connect allows Privilege Escalation.This issue affects Saphira Connect: before 9.	8.8	More Details
CVE-2023-4665	Incorrect Execution-Assigned Permissions vulnerability in Saphira Saphira Connect allows Privilege Escalation.This issue affects Saphira Connect: before 9.	8.8	More Details
CVE-2023-42270	Grocy <= 4.0.2 is vulnerable to Cross Site Request Forgery (CSRF).	8.8	More Details
CVE-2023-40221	The absence of filters when loading some sections in the web application of the vulnerable device allows potential attackers to inject malicious code that will be interpreted when a legitimate user accesses the web section (MAIL SERVER) where the information is displayed. Injection can be done on parameter MAIL_RCV. When a legitimate user attempts to review NOTIFICATION/MAIL SERVER, the injected code will be executed.	8.8	More Details
CVE-2023-40955	A SQL injection vulnerability in Didotech srl Engineering & Lifecycle Management (aka pdm) v.14.0, v.15.0 and v.16.0 fixed in pdm-14.0.1.0.0, pdm-15.0.1.0.0, and pdm-16.0.1.0.0 allows a remote authenticated attacker to execute arbitrary code via the select parameter in models/base_client.py component.	8.8	More Details
CVE-2023-42328	An issue in PeppermintLabs Peppermint v.0.2.4 and before allows a remote attacker to obtain sensitive information and execute arbitrary code via the hardcoded session cookie.	8.8	More Details
CVE-2023-0923	A flaw was found in the Kubernetes service for notebooks in RHODS, where it does not prevent pods from other namespaces and applications from making requests to the Jupyter API. This flaw can lead to file content exposure and other issues.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4153	The BAN Users plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 1.5.3 due to a missing capability check on the 'w3dev_save_ban_user_settings_callback' function. This makes it possible for authenticated attackers, with minimal permissions such as a subscriber, to modify the plugin settings to access the ban and unban functionality and set the role of the unbanned user.	8.8	More Details
CVE-2023-43115	In Artifex Ghostscript through 10.01.2, gdevijs.c in GhostPDL can lead to remote code execution via crafted PostScript documents because they can switch to the IJS device, or change the IjsServer parameter, after SAFER has been activated. NOTE: it is a documented risk that the IJS server can be specified on a gs command line (the IJS device inherently must execute a command to start the IJS server).	8.8	More Details
CVE-2023-42180	An arbitrary file upload vulnerability in the /user/upload component of lenosp 1.0-1.2.0 allows attackers to execute html code via a crafted JPG file.	8.8	More Details
CVE-2023-5036	Cross-Site Request Forgery (CSRF) in GitHub repository usememos/memos prior to 0.15.1.	8.8	More Details
CVE-2023-40956	A SQL injection vulnerability in Cloudroits Website Job Search v.15.0 allows a remote authenticated attacker to execute arbitrary code via the name parameter in controllers/main.py component.	8.8	More Details
CVE-2023-41349	ASUS router RT-AX88U has a vulnerability of using externally controllable format strings within its Advanced Open VPN function. An authenticated remote attacker can exploit the exported OpenVPN configuration to execute an externally-controlled format string attack, resulting in sensitivity information leakage, or forcing the device to reset and permanent denial of service.	8.8	More Details
CVE-2023-38891	SQL injection vulnerability in Vtiger CRM v.7.5.0 allows a remote authenticated attacker to escalate privileges via the getQueryColumnsList function in ReportRun.php.	8.8	More Details
CVE-2023-4213	The Simplr Registration Form Plus+ plugin for WordPress is vulnerable to Insecure Direct Object References in versions up to, and including, 2.4.5. This is due to the plugin providing user-controlled access to objects, letting a user bypass authorization and access system resources. This makes it possible for authenticated attackers with subscriber-level permissions or above to change user passwords and potentially take over administrator accounts.	8.8	More Details
CVE-2023-40868	Cross Site Request Forgery vulnerability in mooSocial MooSocial Software v.Demo allows a remote attacker to execute arbitrary code via the Delete Account and Deactivate functions.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22513	This High severity RCE (Remote Code Execution) vulnerability was introduced in version 8.0.0 of Bitbucket Data Center and Server. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 8.5, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires no user interaction. Atlassian recommends that Bitbucket Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Bitbucket Data Center and Server 8.9: Upgrade to a release greater than or equal to 8.9.5 Bitbucket Data Center and Server 8.10: Upgrade to a release greater than or equal to 8.10.5 Bitbucket Data Center and Server 8.11: Upgrade to a release greater than or equal to 8.11.4 Bitbucket Data Center and Server 8.12: Upgrade to a release greater than or equal to 8.12.2 Bitbucket Data Center and Server 8.13: Upgrade to a release greater than or equal to 8.13.1 Bitbucket Data Center and Server 8.14: Upgrade to a release greater than or equal to 8.14.0 Bitbucket Data Center and Server version >= 8.0 and < 8.9: Upgrade to any of the listed fix versions. See the release notes (https://confluence.atlassian.com/bitbucketserver/release-notes). You can download the latest version of Bitbucket Data Center and Server from the download center (https://www.atlassian.com/software/bitbucket/download-archives). This vulnerability was discovered by a private user and reported via our Bug Bounty program	8.8	More Details
CVE-2023-40933	A SQL injection vulnerability in Nagios XI v5.11.1 and below allows authenticated attackers with announcement banner configuration privileges to execute arbitrary SQL commands via the ID parameter sent to the update_banner_message() function.	8.8	More Details
CVE-2023-4916	The Login with phone number plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.5.6. This is due to missing nonce validation on the 'lwp_update_password_action' function. This makes it possible for unauthenticated attackers to change user password via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2023-42444	phonenumber is a library for parsing, formatting and validating international phone numbers. Prior to versions `0.3.3+8.13.9` and `0.2.5+8.11.3`, the phonenumber parsing code may panic due to a panic-guarded out-of-bounds access on the phonenumber string. In a typical deployment of `rust-phonenumber`, this may get triggered by feeding a maliciously crafted phonenumber over the network, specifically the string `.;phone-context=`. Versions `0.3.3+8.13.9` and `0.2.5+8.11.3` contain a patch for this issue. There are no known workarounds.	8.6	More Details
CVE-2023-4096	Weak password recovery mechanism vulnerability in Fujitsu Arconte Áurea version 1.5.0.0, which exploitation could allow an attacker to perform a brute force attack on the emailed PIN number in order to change the password of a legitimate user.	8.6	More Details
CVE-2023-42447	blurhash-rs is a pure Rust implementation of Blurhash, software for encoding images into ASCII strings that can be turned into a gradient of colors representing the original image. In version 0.1.1, the blurhash parsing code may panic due to multiple panic-guarded out-of-bounds accesses on untrusted input. In a typical deployment, this may get triggered by feeding a maliciously crafted blurhashes over the network. These may include UTF-8 compliant strings containing multi-byte UTF-8 characters. A patch is available in version 0.2.0, which requires user intervention because of slight API churn. No known workarounds are available.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47559	Lack of device control over web requests in ekorCCP and ekorRCI, allowing an attacker to create customised requests to execute malicious actions when a user is logged in, affecting availability, privacy and integrity.	8.6	More Details
CVE-2022-47553	Incorrect authorisation in ekorCCP and ekorRCI, which could allow a remote attacker to obtain resources with sensitive information for the organisation, without being authenticated within the web server.	8.6	More Details
CVE-2023-34999	A command injection vulnerability exists in RTS VLink Virtual Matrix Software Versions v5 (< 5.7.6) and v6 (< 6.5.0) that allows an attacker to perform arbitrary code execution via the admin web interface.	8.4	More Details
CVE-2023-42442	JumpServer is an open source bastion host and a professional operation and maintenance security audit system. Starting in version 3.0.0 and prior to versions 3.5.5 and 3.6.4, session replays can download without authentication. Session replays stored in S3, OSS, or other cloud storage are not affected. The api `/api/v1/terminal/sessions/` permission control is broken and can be accessed anonymously. SessionViewSet permission classes set to `[RBACPermission | IsSessionAssignee]`, relation is or, so any permission matched will be allowed. Versions 3.5.5 and 3.6.4 have a fix. After upgrading, visit the api `$HOST/api/v1/terminal/sessions/?limit=1`. The expected http response code is 401 (`not_authenticated`).	8.2	More Details
CVE-2022-47554	Exposure of sensitive information in ekorCCP and ekorRCI, potentially allowing a remote attacker to obtain critical information from various .xml files, including .xml files containing credentials, without being authenticated within the web server.	8.2	More Details
CVE-2023-38557	A vulnerability has been identified in Spectrum Power 7 (All versions < V23Q3). The affected product assigns improper access rights to the update script. This could allow an authenticated local attacker to inject arbitrary code and escalate privileges.	8.2	More Details
CVE-2023-5009	An issue has been discovered in GitLab EE affecting all versions starting from 13.12 before 16.2.7, all versions starting from 16.3 before 16.3.4. It was possible for an attacker to run pipeline jobs as an arbitrary user via scheduled security scan policies. This was a bypass of [CVE-2023-3932](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-3932) showing additional impact.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42443	Vyper is a Pythonic Smart Contract Language for the Ethereum Virtual Machine (EVM). In version 0.3.9 and prior, under certain conditions, the memory used by the builtins `raw_call`, `create_from_blueprint` and `create_copy_of` can be corrupted. For `raw_call`, the argument buffer of the call can be corrupted, leading to incorrect `calldata` in the sub-context. For `create_from_blueprint` and `create_copy_of`, the buffer for the to-be-deployed bytecode can be corrupted, leading to deploying incorrect bytecode. Each builtin has conditions that must be fulfilled for the corruption to happen. For `raw_call`, the `data` argument of the builtin must be `msg.data` and the `value` or `gas` passed to the builtin must be some complex expression that results in writing to the memory. For `create_copy_of`, the `value` or `salt` passed to the builtin must be some complex expression that results in writing to the memory. For `create_from_blueprint`, either no constructor parameters should be passed to the builtin or `raw_args` should be set to True, and the `value` or `salt` passed to the builtin must be some complex expression that results in writing to the memory. As of time of publication, no patched version exists. The issue is still being investigated, and there might be other cases where the corruption might happen. When the builtin is being called from an `internal` function `F`, the issue is not present provided that the function calling `F` wrote to memory before calling `F`. As a workaround, the complex expressions that are being passed as kwargs to the builtin should be cached in memory prior to the call to the builtin.	8.1	More Details
CVE-2023-38356	MiniTool Power Data Recovery 11.6 contains an insecure installation process that allows attackers to achieve remote code execution through a man in the middle attack.	8.1	More Details
CVE-2023-38355	MiniTool Movie Maker 7.0 contains an insecure installation process that allows attackers to achieve remote code execution through a man in the middle attack.	8.1	More Details
CVE-2023-29245	A SQL Injection vulnerability in Nozomi Networks Guardian and CMC, due to improper input validation in certain fields used in the Asset Intelligence functionality of our IDS, may allow an unauthenticated attacker to execute arbitrary SQL statements on the DBMS used by the web application by sending specially crafted malicious network packets. Malicious users with extensive knowledge on the underlying system may be able to extract arbitrary information from the DBMS in an uncontrolled way, alter its structure and data, and/or affect its availability.	8.1	More Details
CVE-2023-38351	MiniTool Partition Wizard 12.8 contains an insecure installation mechanism that allows attackers to achieve remote code execution through a man in the middle attack.	8.1	More Details
CVE-2023-38354	MiniTool Shadow Maker version 4.1 contains an insecure installation process that allows attackers to achieve remote code execution through a man in the middle attack.	8.1	More Details
CVE-2023-38352	MiniTool Partition Wizard 12.8 contains an insecure update mechanism that allows attackers to achieve remote code execution through a man in the middle attack.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29183	An improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability [CWE-79] in FortiProxy 7.2.0 through 7.2.4, 7.0.0 through 7.0.10 and FortiOS 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.12, 6.2.0 through 6.2.14 GUI may allow an authenticated attacker to trigger malicious JavaScript code execution via crafted guest management setting.	8.0	More Details
CVE-2023-2848	Movim prior to version 0.22 is affected by a Cross-Site WebSocket Hijacking vulnerability. This was the result of a missing header validation.	8.0	More Details
CVE-2023-36250	CSV Injection vulnerability in GNOME time tracker version 3.0.2, allows local attackers to execute arbitrary code via crafted .tsv file when creating a new record.	7.8	More Details
CVE-2023-41267	In the Apache Airflow HDFS Provider, versions prior to 4.1.1, a documentation info pointed users to an install incorrect pip package. As this package name was unclaimed, in theory, an attacker could claim this package and provide code that would be executed when this package was installed. The Airflow team has since taken ownership of the package (neutralizing the risk), and fixed the doc strings in version 4.1.1	7.8	More Details
CVE-2023-4516	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the IGSS Update Service that could allow a local attacker to change update source, potentially leading to remote code execution when the attacker force an update containing malicious content.	7.8	More Details
CVE-2022-35849	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the management interface of FortiADC 7.1.0 through 7.1.1, 7.0.0 through 7.0.3, 6.2.0 through 6.2.5 and 6.1.0 all versions may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands.	7.8	More Details
CVE-2023-36658	An issue was discovered in OPSWAT MetaDefender KIOSK 4.6.1.9996. It has an unquoted service path that can be abused locally.	7.8	More Details
CVE-2023-4991	A vulnerability was found in NextBX QWAlerter 4.50. It has been rated as critical. Affected by this issue is some unknown functionality of the file QWAlerter.exe. The manipulation leads to unquoted search path. It is possible to launch the attack on the local host. The identifier of this vulnerability is VDB-239804. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.8	More Details
CVE-2022-47631	Razer Synapse through 3.7.1209.121307 allows privilege escalation due to an unsafe installation path and improper privilege management. Attackers can place DLLs into %PROGRAMDATA%\Razer\Synapse3\Service\bin if they do so before the service is installed and if they deny write access for the SYSTEM user. Although the service will not start if it detects malicious DLLs in this directory, attackers can exploit a race condition and replace a valid DLL (i.e., a copy of a legitimate Razer DLL) with a malicious DLL after the service has already checked the file. As a result, local Windows users can abuse the Razer driver installer to obtain administrative privileges on Windows.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34195	An issue was discovered in SystemFirmwareManagementRuntimeDxe in Insyde InsydeH2O with kernel 5.0 through 5.5. The implementation of the GetImage method retrieves the value of a runtime variable named GetImageProgress, and later uses this value as a function pointer. This variable is wiped out by the same module near the end of the function. By setting this UEFI variable from the OS to point into custom code, an attacker could achieve arbitrary code execution in the DXE phase, before several chipset locks are set.	7.8	More Details
CVE-2023-26369	Acrobat Reader versions 23.003.20284 (and earlier), 20.005.30516 (and earlier) and 20.005.30514 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-32184	A Insecure Storage of Sensitive Information vulnerability in openSUSE opensuse-welcome allows local attackers to execute code as the user that runs opensuse-welcome if a custom layout is chosen This issue affects opensuse-welcome: from 0.1 before 0.1.9+git.35.4b9444a.	7.8	More Details
CVE-2023-38205	Adobe ColdFusion versions 2018u18 (and earlier), 2021u8 (and earlier) and 2023u2 (and earlier) are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to access the administration CFM and CFC endpoints. Exploitation of this issue does not require user interaction.	7.5	More Details
CVE-2023-42439	GeoNode is an open source platform that facilitates the creation, sharing, and collaborative use of geospatial data. A SSRF vulnerability exists starting in version 3.2.0, bypassing existing controls on the software. This can allow a user to request internal services for a full read SSRF, returning any data from the internal network. The application is using a whitelist, but the whitelist can be bypassed. The bypass will trick the application that the first host is a whitelisted address, but the browser will use `@` or `%40` as a credential to the host geoserver on port 8080, this will return the data to that host on the response. Version 4.1.3.post1 is the first available version that contains a patch.	7.5	More Details
CVE-2023-41886	OpenRefine is a powerful free, open source tool for working with messy data. Prior to version 3.7.5, an arbitrary file read vulnerability allows any unauthenticated user to read a file on a server. Version 3.7.5 fixes this issue.	7.5	More Details
CVE-2023-38039	When curl retrieves an HTTP response, it stores the incoming headers so that they can be accessed later via the libcurl headers API. However, curl did not have a limit in how many or how large headers it would accept in a response, allowing a malicious server to stream an endless series of headers and eventually cause curl to run out of heap memory.	7.5	More Details
CVE-2023-1108	A flaw was found in undertow. This issue makes achieving a denial of service possible due to an unexpected handshake status updated in SslConduit, where the loop never terminates.	7.5	More Details
CVE-2023-0813	A flaw was found in the Network Observability plugin for OpenShift console. Unless the Loki authToken configuration is set to FORWARD mode, authentication is no longer enforced, allowing any user who can connect to the OpenShift Console in an OpenShift cluster to retrieve flows without authentication.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40019	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.10.10, FreeSWITCH allows authorized users to cause a denial of service attack by sending re-INVITE with SDP containing duplicate codec names. When a call in FreeSWITCH completes codec negotiation, the `codec_string` channel variable is set with the result of the negotiation. On a subsequent re-negotiation, if an SDP is offered that contains codecs with the same names but with different formats, there may be too many codec matches detected by FreeSWITCH leading to overflows of its internal arrays. By abusing this vulnerability, an attacker is able to corrupt stack of FreeSWITCH leading to an undefined behavior of the system or simply crash it. Version 1.10.10 contains a patch for this issue.	7.5	More Details
CVE-2023-40018	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.10.10, FreeSWITCH allows remote users to trigger out of bounds write by offering an ICE candidate with unknown component ID. When an SDP is offered with any ICE candidates with an unknown component ID, FreeSWITCH will make an out of bounds write to its arrays. By abusing this vulnerability, an attacker is able to corrupt FreeSWITCH memory leading to an undefined behavior of the system or a crash of it. Version 1.10.10 contains a patch for this issue.	7.5	More Details
CVE-2023-35851	SUNNET WMPro portal's FAQ function has insufficient validation for user input. An unauthenticated remote attacker can inject arbitrary SQL commands to obtain sensitive information via a database.	7.5	More Details
CVE-2022-47848	An issue was discovered in Bezeq Vtech NB403-IL version BZ_2.02.07.09.13.01 and Vtech IAD604-IL versions BZ_2.02.07.09.13.01, BZ_2.02.07.09.13T, and BZ_2.02.07.09.09T, allows remote attackers to gain sensitive information via rootDesc.xml page of the UPnP service.	7.5	More Details
CVE-2023-32187	An Allocation of Resources Without Limits or Throttling vulnerability in SUSE k3s allows attackers with access to K3s servers' apiserver/supervisor port (TCP 6443) cause denial of service. This issue affects k3s: from v1.24.0 before v1.24.17+k3s1, from v1.25.0 before v1.25.13+k3s1, from v1.26.0 before v1.26.8+k3s1, from sev1.27.0 before v1.27.5+k3s1, from v1.28.0 before v1.28.1+k3s1.	7.5	More Details
CVE-2023-26141	Versions of the package sidekiq before 7.1.3 are vulnerable to Denial of Service (DoS) due to insufficient checks in the dashboard-charts.js file. An attacker can exploit this vulnerability by manipulating the localStorage value which will cause excessive polling requests.	7.5	More Details
CVE-2023-41595	An issue in xui-xray v1.8.3 allows attackers to obtain sensitive information via default password.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41081	Important: Authentication Bypass CVE-2023-41081 The mod_jk component of Apache Tomcat Connectors in some circumstances, such as when a configuration included "JkOptions +ForwardDirectories" but the configuration did not provide explicit mounts for all possible proxied requests, mod_jk would use an implicit mapping and map the request to the first defined worker. Such an implicit mapping could result in the unintended exposure of the status worker and/or bypass security constraints configured in httpd. As of JK 1.2.49, the implicit mapping functionality has been removed and all mappings must now be via explicit configuration. Only mod_jk is affected by this issue. The ISAPI redirector is not affected. This issue affects Apache Tomcat Connectors (mod_jk only): from 1.2.0 through 1.2.48. Users are recommended to upgrade to version 1.2.49, which fixes the issue. History 2023-09-13 Original advisory 2023-09-28 Updated summary	7.5	More Details
CVE-2023-34984	A protection mechanism failure in Fortinet FortiWeb 7.2.0 through 7.2.1, 7.0.0 through 7.0.6, 6.4.0 through 6.4.3, 6.3.6 through 6.3.23 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests.	7.5	More Details
CVE-2023-41890	Sustainsys.Saml2 library adds SAML2P support to ASP.NET web sites, allowing the web site to act as a SAML2 Service Provider. Prior to versions 1.0.3 and 2.9.2, when a response is processed, the issuer of the Identity Provider is not sufficiently validated. This could allow a malicious identity provider to craft a Saml2 response that is processed as if issued by another identity provider. It is also possible for a malicious end user to cause stored state intended for one identity provider to be used when processing the response from another provider. An application is impacted if they rely on any of these features in their authentication/authorization logic: the issuer of the generated identity and claims; or items in the stored request state (AuthenticationProperties). This issue is patched in versions 2.9.2 and 1.0.3. The `AcsCommandResultCreated` notification can be used to add the validation required if an upgrade to patched packages is not possible.	7.5	More Details
CVE-2023-39914	NLnet Labs' bcder library up to and including version 0.7.2 panics while decoding certain invalid input data rather than rejecting the data with an error. This can affect both the actual decoding stage as well as accessing content of types that utilized delayed decoding.	7.5	More Details
CVE-2023-39915	NLnet Labs' Routinator up to and including version 0.12.1 may crash when trying to parse certain malformed RPKI objects. This is due to insufficient input checking in the bcder library covered by CVE-2023-39914.	7.5	More Details
CVE-2023-4801	An improper certification validation vulnerability in the Insider Threat Management (ITM) Agent for MacOS could be used by an anonymous actor on an adjacent network to establish a man-in-the-middle position between the agent and the ITM server after the agent has registered. All versions prior to 7.14.3.69 are affected. Agents for Windows, Linux, and Cloud are unaffected.	7.5	More Details
CVE-2023-32649	A Denial of Service (Dos) vulnerability in Nozomi Networks Guardian and CMC, due to improper input validation in certain fields used in the Asset Intelligence functionality of our IDS, allows an unauthenticated attacker to crash the IDS module by sending specially crafted malformed network packets. During the (limited) time window before the IDS module is automatically restarted, network traffic may not be analyzed.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32186	A Allocation of Resources Without Limits or Throttling vulnerability in SUSE RKE2 allows attackers with access to K3s servers apiserver/supervisor port (TCP 6443) cause denial of service. This issue affects RKE2: from 1.24.0 before 1.24.17+rke2r1, from v1.25.0 before v1.25.13+rke2r1, from v1.26.0 before v1.26.8+rke2r1, from v1.27.0 before v1.27.5+rke2r1, from v1.28.0 before v1.28.1+rke2r1.	7.5	More Details
CVE-2023-2680	This CVE exists because of an incomplete fix for CVE-2021-3750. More specifically, the qemu-kvm package as released for Red Hat Enterprise Linux 9.1 via RHSA-2022:7967 included a version of qemu-kvm that was actually missing the fix for CVE-2021-3750.	7.5	More Details
CVE-2023-39452	The web application that owns the device clearly stores the credentials within the user management section. Obtaining this information can be done remotely due to the incorrect management of the sessions in the web application.	7.5	More Details
CVE-2023-42520	Certain WithSecure products allow a remote crash of a scanning engine via unpacking of crafted data files. This affects WithSecure Client Security 15, WithSecure Server Security 15, WithSecure Email and Server Security 15, WithSecure Elements Endpoint Protection 17 and later, WithSecure Client Security for Mac 15, WithSecure Elements Endpoint Protection for Mac 17 and later, Linux Security 64 12.0 , Linux Protection 12.0, and WithSecure Atlant (formerly F-Secure Atlant) 1.0.35-1.	7.5	More Details
CVE-2023-4785	Lack of error handling in the TCP server in Google's gRPC starting version 1.23 on posix-compatible platforms (ex. Linux) allows an attacker to cause a denial of service by initiating a significant number of connections with the server. Note that gRPC C++ Python, and Ruby are affected, but gRPC Java, and Go are NOT affected.	7.5	More Details
CVE-2023-41965	Sending some requests in the web application of the vulnerable device allows information to be obtained due to the lack of security in the authentication process.	7.5	More Details
CVE-2023-40850	netentsec NS-ASG 6.3 is vulnerable to Incorrect Access Control. There is a file leak in the website source code of the application security gateway.	7.5	More Details
CVE-2023-42524	Certain WithSecure products allow an infinite loop in a scanning engine via unspecified file types. This affects WithSecure Client Security 15, WithSecure Server Security 15, WithSecure Email and Server Security 15, WithSecure Elements Endpoint Protection 17 and later, WithSecure Client Security for Mac 15, WithSecure Elements Endpoint Protection for Mac 17 and later, Linux Security 64 12.0 , Linux Protection 12.0, and WithSecure Atlant (formerly F-Secure Atlant) 1.0.35-1.	7.5	More Details
CVE-2023-42526	Certain WithSecure products allow a remote crash of a scanning engine via decompression of crafted data files. This affects WithSecure Client Security 15, WithSecure Server Security 15, WithSecure Email and Server Security 15, WithSecure Elements Endpoint Protection 17 and later, WithSecure Client Security for Mac 15, WithSecure Elements Endpoint Protection for Mac 17 and later, Linux Security 64 12.0 , Linux Protection 12.0, and WithSecure Atlant (formerly F-Secure Atlant) 1.0.35-1.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42521	Certain WithSecure products allow a remote crash of a scanning engine via processing of a compressed file. This affects WithSecure Client Security 15, WithSecure Server Security 15, WithSecure Email and Server Security 15, WithSecure Elements Endpoint Protection 17 and later, WithSecure Client Security for Mac 15, WithSecure Elements Endpoint Protection for Mac 17 and later, Linux Security 64 12.0 , Linux Protection 12.0, and WithSecure Atlant (formerly F-Secure Atlant) 1.0.35-1.	7.5	More Details
CVE-2023-42523	Certain WithSecure products allow a remote crash of a scanning engine via unpacking of a PE file. This affects WithSecure Client Security 15, WithSecure Server Security 15, WithSecure Email and Server Security 15, WithSecure Elements Endpoint Protection 17 and later, WithSecure Client Security for Mac 15, WithSecure Elements Endpoint Protection for Mac 17 and later, Linux Security 64 12.0 , Linux Protection 12.0, and WithSecure Atlant (formerly F-Secure Atlant) 1.0.35-1.	7.5	More Details
CVE-2023-42522	Certain WithSecure products allow a remote crash of a scanning engine via processing of an import struct in a PE file. This affects WithSecure Client Security 15, WithSecure Server Security 15, WithSecure Email and Server Security 15, WithSecure Elements Endpoint Protection 17 and later, WithSecure Client Security for Mac 15, WithSecure Elements Endpoint Protection for Mac 17 and later, Linux Security 64 12.0 , Linux Protection 12.0, and WithSecure Atlant (formerly F-Secure Atlant) 1.0.35-1.	7.5	More Details
CVE-2023-42525	Certain WithSecure products allow an infinite loop in a scanning engine via unspecified file types. This affects WithSecure Client Security 15, WithSecure Server Security 15, WithSecure Email and Server Security 15, WithSecure Elements Endpoint Protection 17 and later, WithSecure Client Security for Mac 15, WithSecure Elements Endpoint Protection for Mac 17 and later, Linux Security 64 12.0 , Linux Protection 12.0, and WithSecure Atlant (formerly F-Secure Atlant) 1.0.35-1.	7.5	More Details
CVE-2023-42387	An issue in TDSQL Chitu management platform v.10.3.19.5.0 allows a remote attacker to obtain sensitive information via get_db_info function in install.php.	7.5	More Details
CVE-2023-41325	OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone technology. Starting in version 3.20 and prior to version 3.22, `shdr_verify_signature` can make a double free. `shdr_verify_signature` used to verify a TA binary before it is loaded. To verify a signature of it, allocate a memory for RSA key. RSA key allocate function (`sw_crypto_acipher_alloc_rsa_public_key`) will try to allocate a memory (which is optee's heap memory). RSA key is consist of exponent and modulus (represent as variable `e`, `n`) and it allocation is not atomic way, so it may succeed in `e` but fail in `n`. In this case sw_crypto_acipher_alloc_rsa_public_key` will free on `e` and return as it is failed but variable 'e' is remained as already freed memory address . `shdr_verify_signature` will free again that memory (which is `e`) even it is freed when it failed allocate RSA key. A patch is available in version 3.22. No known workarounds are available.	7.4	More Details
CVE-2023-42451	Mastodon is a free, open-source social network server based on ActivityPub. Prior to versions 3.5.14, 4.0.10, 4.1.8, and 4.2.0-rc2, under certain circumstances, attackers can exploit a flaw in domain name normalization to spoof domains they do not own. Versions 3.5.14, 4.0.10, 4.1.8, and 4.2.0-rc2 contain a patch for this issue.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38507	Strapi is the an open-source headless content management system. Prior to version 4.12.1, there is a rate limit on the login function of Strapi's admin screen, but it is possible to circumvent it. Therefore, the possibility of unauthorized login by login brute force attack increases. Version 4.12.1 has a fix for this issue.	7.3	More Details
CVE-2023-5020	A vulnerability, which was classified as critical, has been found in 07FLY CRM V2. This issue affects some unknown processing of the file /index.php/sysmanage/Login/login_auth/ of the component Administrator Login Page. The manipulation of the argument account leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-239861 was assigned to this vulnerability.	7.3	More Details
CVE-2023-3891	Race condition in Lapce v0.2.8 allows an attacker to elevate privileges on the system	7.3	More Details
CVE-2023-41929	A DLL hijacking vulnerability in Samsung Memory Card & UFD Authentication Utility PC Software before 1.0.1 could allow a local attacker to escalate privileges. (An attacker must already have user privileges on Windows to exploit this vulnerability.)	7.3	More Details
CVE-2023-41443	SQL injection vulnerability in Novel-Plus v.4.1.0 allows a remote attacker to execute arbitrary code via a crafted script to the sort parameter in /sys/menu/list.	7.2	More Details
CVE-2023-3025	The Dropbox Folder Share plugin for WordPress is vulnerable to Server-Side Request Forgery in versions up to, and including, 1.9.7 via the 'link' parameter. This can allow unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	7.2	More Details
CVE-2023-31808	Technicolor TG670 10.5.N.9 devices contain multiple accounts with hard-coded passwords. One account has administrative privileges, allowing for unrestricted access over the WAN interface if Remote Administration is enabled.	7.2	More Details
CVE-2023-41179	A vulnerability in the 3rd party AV uninstaller module contained in Trend Micro Apex One (on-prem and SaaS), Worry-Free Business Security and Worry-Free Business Security Services could allow an attacker to manipulate the module to execute arbitrary commands on an affected installation. Note that an attacker must first obtain administrative console access on the target system in order to exploit this vulnerability.	7.2	More Details
CVE-2023-35850	SUNNET WMPro portal's file management function has a vulnerability of insufficient filtering for user input. A remote attacker with administrator privilege or a privileged account can exploit this vulnerability to inject and execute arbitrary system commands to perform arbitrary system operations or disrupt service.	7.2	More Details
CVE-2023-4928	SQL Injection in GitHub repository instantsoft/icms2 prior to 2.16.1.	7.2	More Details
CVE-2023-40934	A SQL injection vulnerability in Nagios XI 5.11.1 and below allows authenticated attackers with privileges to manage host escalations in the Core Configuration Manager to execute arbitrary SQL commands via the host escalation notification settings.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36634	An incomplete filtering of one or more instances of special elements vulnerability [CWE-792] in the command line interpreter of FortiAP-U 7.0.0, 6.2.0 through 6.2.5, 6.0 all versions, 5.4 all versions may allow an authenticated attacker to list and delete arbitrary files and directory via specially crafted command arguments.	7.1	More Details
CVE-2023-36562	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	7.1	More Details
CVE-2023-4814	A Privilege escalation vulnerability exists in Trellix Windows DLP endpoint for windows which can be abused to delete any file/folder for which the user does not have permission to.	7.1	More Details
CVE-2023-4680	HashiCorp Vault and Vault Enterprise transit secrets engine allowed authorized users to specify arbitrary nonces, even with convergent encryption disabled. The encrypt endpoint, in combination with an offline attack, could be used to decrypt arbitrary ciphertext and potentially derive the authentication subkey when using transit secrets engine without convergent encryption. Introduced in 1.6.0 and fixed in 1.14.3, 1.13.7, and 1.12.11.	6.8	More Details
CVE-2023-37263	Strapi is the an open-source headless content management system. Prior to version 4.12.1, field level permissions are not respected in the relationship title. If an actor has relationship title and the relationship shows a field they don't have permission to see, the field will still be visible. Version 4.12.1 has a fix for this issue.	6.8	More Details
CVE-2023-23845	The SolarWinds Platform was susceptible to the Incorrect Comparison Vulnerability. This vulnerability allows users with administrative access to SolarWinds Web Console to execute arbitrary commands with NETWORK SERVICE privileges.	6.8	More Details
CVE-2023-23840	The SolarWinds Platform was susceptible to the Incorrect Comparison Vulnerability. This vulnerability allows users with administrative access to SolarWinds Web Console to execute arbitrary commands with NETWORK SERVICE privileges.	6.8	More Details
CVE-2023-36642	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the management interface of FortiTester 3.0.0 through 7.2.3 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands.	6.7	More Details
CVE-2023-20236	A vulnerability in the iPXE boot function of Cisco IOS XR software could allow an authenticated, local attacker to install an unverified software image on an affected device. This vulnerability is due to insufficient image verification. An attacker could exploit this vulnerability by manipulating the boot parameters for image verification during the iPXE boot process on an affected device. A successful exploit could allow the attacker to boot an unverified software image on the affected device.	6.7	More Details
CVE-2023-42178	Lenosp 1.0.0-1.2.0 is vulnerable to SQL Injection via the log query module.	6.5	More Details
CVE-2023-39039	An information leak in Camp Style Project Line v13.6.1 allows attackers to obtain the channel access token and send crafted messages.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39040	An information leak in Cheese Cafe Line v13.6.1 allows attackers to obtain the channel access token and send crafted messages.	6.5	More Details
CVE-2023-39043	An information leak in YKC Tokushima_awayokocho Line v13.6.1 allows attackers to obtain the channel access token and send crafted messages.	6.5	More Details
CVE-2023-4959	A flaw was found in Quay. Cross-site request forgery (CSRF) attacks force a user to perform unwanted actions in an application. During the pentest, it was detected that the config-editor page is vulnerable to CSRF. The config-editor page is used to configure the Quay instance. By coercing the victim's browser into sending an attacker-controlled request from another domain, it is possible to reconfigure the Quay instance (including adding users with admin privileges).	6.5	More Details
CVE-2023-39058	An information leak in THE_B_members card v13.6.1 allows attackers to obtain the channel access token and send crafted messages.	6.5	More Details
CVE-2022-47556	Uncontrolled resource consumption in ekorRCI, allowing an attacker with low-privileged access to the web server to send continuous legitimate web requests to a functionality that is not properly validated, in order to cause a denial of service (DoS) on the device.	6.5	More Details
CVE-2023-4094	ARCONTE Aurea's authentication system, in its 1.5.0.0 version, could allow an attacker to make incorrect access requests in order to block each legitimate account and cause a denial of service. In addition, a resource has been identified that could allow circumventing the attempt limit set in the login form.	6.5	More Details
CVE-2023-39046	An information leak in TonTon-Tei_waiting Line v13.6.1 allows attackers to obtain the channel access token and send crafted messages.	6.5	More Details
CVE-2023-39049	An information leak in youmart-tokunaga v13.6.1 allows attackers to obtain the channel access token and send crafted messages.	6.5	More Details
CVE-2023-39056	An information leak in Coffee-jumbo v13.6.1 allows attackers to obtain the channel access token and send crafted messages.	6.5	More Details
CVE-2023-42446	Pow is a authentication and user management solution for Phoenix and Plug-based apps. Starting in version 1.0.14 and prior to version 1.0.34, use of `Pow.Store.Backend.MnesiaCache` is susceptible to session hijacking as expired keys are not being invalidated correctly on startup. A session may expire when all `Pow.Store.Backend.MnesiaCache` instances have been shut down for a period that is longer than a session's remaining TTL. Version 1.0.34 contains a patch for this issue. As a workaround, expired keys, including all expired sessions, can be manually invalidated.	6.5	More Details
CVE-2023-26143	Versions of the package blamer before 1.0.4 are vulnerable to Arbitrary Argument Injection via the blameByFile() API. The library does not sanitize for user input or validate the given file path conforms to a specific schema, nor does it properly pass command-line flags to the git binary using the double-dash POSIX characters (--) to communicate the end of options.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3255	A flaw was found in the QEMU built-in VNC server while processing ClientCutText messages. A wrong exit condition may lead to an infinite loop when inflating an attacker controlled zlib buffer in the `inflate_buffer` function. This could allow a remote authenticated client who is able to send a clipboard to the VNC server to trigger a denial of service.	6.5	More Details
CVE-2023-38255	A potential attacker with or without (cookie theft) access to the device would be able to include malicious code (XSS) when uploading new device configuration that could affect the intended function of the device.	6.5	More Details
CVE-2023-41043	Discourse is an open-source discussion platform. Prior to version 3.1.1 of the `stable` branch and version 3.2.0.beta1 of the `beta` and `tests-passed` branches, a malicious admin could create extremely large icons sprites, which would then be cached in each server process. This may cause server processes to be killed and lead to downtime. The issue is patched in version 3.1.1 of the `stable` branch and version 3.2.0.beta1 of the `beta` and `tests-passed` branches. This is only a concern for multisite installations. No action is required when the admins are trusted.	6.5	More Details
CVE-2023-40588	Discourse is an open-source discussion platform. Prior to version 3.1.1 of the `stable` branch and version 3.2.0.beta1 of the `beta` and `tests-passed` branches, a malicious user could add a 2FA or security key with a carefully crafted name to their account and cause a denial of service for other users. The issue is patched in version 3.1.1 of the `stable` branch and version 3.2.0.beta1 of the `beta` and `tests-passed` branches. There are no known workarounds.	6.5	More Details
CVE-2023-4527	A flaw was found in glibc. When the getaddrinfo function is called with the AF_UNSPEC address family and the system is configured with no-aaaa mode via /etc/resolv.conf, a DNS response via TCP larger than 2048 bytes can potentially disclose stack contents through the function returned address data, and may cause a crash.	6.5	More Details
CVE-2023-38706	Discourse is an open-source discussion platform. Prior to version 3.1.1 of the `stable` branch and version 3.2.0.beta1 of the `beta` and `tests-passed` branches, a malicious user can create an unlimited number of drafts with very long draft keys which may end up exhausting the resources on the server. The issue is patched in version 3.1.1 of the `stable` branch and version 3.2.0.beta1 of the `beta` and `tests-passed` branches. There are no known workarounds.	6.5	More Details
CVE-2023-37739	i-doit Pro v25 and below was discovered to be vulnerable to path traversal.	6.5	More Details
CVE-2023-4568	PaperCut NG allows for unauthenticated XMLRPC commands to be run by default. Versions 22.0.12 and below are confirmed to be affected, but later versions may also be affected due to lack of a vendor supplied patch.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40931	A SQL injection vulnerability in Nagios XI from version 5.11.0 up to and including 5.11.1 allows authenticated attackers to execute arbitrary SQL commands via the ID parameter in the POST request to /nagiosxi/admin/banner_message-ajaxhelper.php	6.5	More Details
CVE-2023-4944	The Awesome Weather Widget for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'awesome-weather' shortcode in versions up to, and including, 3.0.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-4945	The Booster for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple shortcodes in versions up to, and including, 7.1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5001	The Horizontal scrolling announcement for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'horizontal-scrolling' shortcode in versions up to, and including, 9.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-4841	The Feeds for YouTube for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'youtube-feed' shortcode in versions up to, and including, 2.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-4963	The WS Facebook Like Box Widget for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'ws-facebook-likebox' shortcode in versions up to, and including, 5.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-4828	An improper check for an exceptional condition in the Insider Threat Management (ITM) Server could be used by an attacker to change the server's configuration of any already-registered agent so that the agent sends all future communications to an attacker-chosen URL. This could result in disclosure of sensitive data events from the agent about the personally identifiable information (PII) and intellectual property it monitors, and all such data could be altered or deleted before reaching the ITM Server. An attacker must first successfully obtain valid agent credentials and agent hostname. All versions prior to 7.14.3.69 are affected.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38582	Persistent cross-site scripting (XSS) in the web application of MOD3GP-SY-120K allows an authenticated remote attacker to introduce arbitrary JavaScript by injecting an XSS payload into the field MAIL_RCV. When a legitimate user attempts to access to the vulnerable page of the web application, the XSS payload will be executed.	6.3	More Details
CVE-2023-5034	A vulnerability classified as problematic was found in SourceCodester My Food Recipe 1.0. This vulnerability affects unknown code of the file index.php of the component Image Upload Handler. The manipulation leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-239878 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-5019	A vulnerability classified as critical was found in Tongda OA. This vulnerability affects unknown code of the file general/hr/manage/staff_reinstatement/delete.php. The manipulation of the argument REINSTATEMENT_ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-239860.	6.3	More Details
CVE-2023-5031	A vulnerability was found in OpenRapid RapidCMS 1.3.1. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/article/article-add.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-239875.	6.3	More Details
CVE-2023-5032	A vulnerability was found in OpenRapid RapidCMS 1.3.1. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/article/article-edit-run.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-239876.	6.3	More Details
CVE-2023-5027	A vulnerability classified as critical was found in SourceCodester Simple Membership System 1.0. Affected by this vulnerability is an unknown functionality of the file club_validator.php. The manipulation of the argument club leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-239869 was assigned to this vulnerability.	6.3	More Details
CVE-2023-25584	An out-of-bounds read flaw was found in the parse_module function in bfd/vms-alpha.c in Binutils.	6.3	More Details
CVE-2023-41030	Hard-coded credentials in Juplink RX4-1500 versions V1.0.2 through V1.0.5 allow unauthenticated attackers to log in to the web interface or telnet service as the 'user' user.	6.3	More Details
CVE-2023-5018	A vulnerability classified as critical has been found in SourceCodester Lost and Found Information System 1.0. This affects an unknown part of the file /classes/Master.php?f=save_category of the component POST Parameter Handler. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-239859.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5033	A vulnerability classified as critical has been found in OpenRapid RapidCMS 1.3.1. This affects an unknown part of the file /admin/category/cate-edit-run.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-239877 was assigned to this vulnerability.	6.3	More Details
CVE-2023-4974	A vulnerability was found in Academy LMS 6.2. It has been rated as critical. Affected by this issue is some unknown functionality of the file /academy/tutor/filter of the component GET Parameter Handler. The manipulation of the argument price_min/price_max leads to sql injection. The attack may be launched remotely. VDB-239750 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-5016	A vulnerability was found in spider-flow up to 0.5.0. It has been declared as critical. Affected by this vulnerability is the function DriverManager.getConnection of the file src/main/java/org/spiderflow/controller/DataSourceController.java of the component API. The manipulation leads to deserialization. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-239857 was assigned to this vulnerability.	6.3	More Details
CVE-2023-5014	A vulnerability was found in Sakshi2610 Food Ordering Website 1.0 and classified as critical. This issue affects some unknown processing of the file categoryfood.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-239855.	6.3	More Details
CVE-2023-4988	A vulnerability, which was classified as problematic, was found in Bettershop LaikeTui. This affects an unknown part of the file index.php?module=system&action=uploadImg. The manipulation of the argument imgFile leads to unrestricted upload. It is possible to initiate the attack remotely. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The associated identifier of this vulnerability is VDB-239799.	6.3	More Details
CVE-2023-4400	A password management vulnerability in Skyhigh Secure Web Gateway (SWG) in main releases 11.x prior to 11.2.14, 10.x prior to 10.2.25 and controlled release 12.x prior to 12.2.1, allows some authentication information stored in configuration files to be extracted through SWG REST API. This was possible due to SWG storing the password in plain text in some configuration files.	6.2	More Details
CVE-2023-5060	Cross-site Scripting (XSS) - DOM in GitHub repository librenms/librenms prior to 23.9.1.	6.1	More Details
CVE-2023-36727	Microsoft Edge (Chromium-based) Spoofing Vulnerability	6.1	More Details
CVE-2023-4978	Cross-site Scripting (XSS) - DOM in GitHub repository librenms/librenms prior to 23.9.0.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42399	Cross Site Scripting vulnerability in xdsoft.net Jodit Editor v.4.0.0-beta.86 allows a remote attacker to obtain sensitive information via the rich text editor component.	6.1	More Details
CVE-2023-40617	A reflected cross-site scripting (XSS) vulnerability in OpenKnowledgeMaps Head Start 7 allows remote attackers to execute arbitrary JavaScript in the web browser of a user, by including a malicious payload into the 'file' parameter in 'displayPDF.php'.	6.1	More Details
CVE-2023-42253	Code-Projects Vehicle Management 1.0 is vulnerable to Cross Site Scripting (XSS) in Add Accounts via Invoice No, To, and Mammul.	6.1	More Details
CVE-2023-41588	A cross-site scripting (XSS) vulnerability in Time to SLA plugin v10.13.5 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the durationFormat parameter.	6.1	More Details
CVE-2023-4663	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Saphira Saphira Connect allows Reflected XSS.This issue affects Saphira Connect: before 9.	6.1	More Details
CVE-2023-40779	An issue in IceWarp Mail Server Deep Castle 2 v.13.0.1.2 allows a remote attacker to execute arbitrary code via a crafted request to the URL.	6.1	More Details
CVE-2022-47557	Vulnerability in ekorCCP and ekorRCI that could allow an attacker with access to the network where the device is located to decrypt the credentials of privileged users, and subsequently gain access to the system to perform malicious actions.	6.1	More Details
CVE-2023-41834	Improper Neutralization of CRLF Sequences in HTTP Headers in Apache Flink Stateful Functions 3.1.0, 3.1.1 and 3.2.0 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via crafted HTTP requests. Attackers could potentially inject malicious content into the HTTP response that is sent to the user's browser. Users should upgrade to Apache Flink Stateful Functions version 3.3.0.	6.1	More Details
CVE-2023-40869	Cross Site Scripting vulnerability in mooSocial mooSocial Software 3.1.6 and 3.1.7 allows a remote attacker to execute arbitrary code via a crafted script to the edit_menu, copuon, and group_categorias functions.	6.1	More Details
CVE-2023-29306	Adobe Connect versions 12.3 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	6.1	More Details
CVE-2023-41162	A Reflected Cross-site scripting (XSS) vulnerability in the file manager tab in Usermin 2.000 allows remote attackers to inject arbitrary web script or HTML via the file mask field while searching under the tools drop down.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42452	Mastodon is a free, open-source social network server based on ActivityPub. In versions on the 4.x branch prior to versions 4.0.10, 4.2.8, and 4.2.0-rc2, under certain conditions, attackers can abuse the translation feature to bypass the server-side HTML sanitization, allowing unescaped HTML to execute in the browser. The impact is limited thanks to Mastodon's strict Content Security Policy, blocking inline scripts, etc. However a CSP bypass or loophole could be exploited to execute malicious XSS. Furthermore, it requires user interaction, as this can only occur upon clicking the “Translate” button on a malicious post. Versions 4.0.10, 4.2.8, and 4.2.0-rc2 contain a patch for this issue.	6.1	More Details
CVE-2023-38040	A reflected XSS vulnerability exists in Revive Adserver 5.4.1 and earlier versions..	6.1	More Details
CVE-2023-4676	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Yordam MedasPro allows Reflected XSS.This issue affects MedasPro: before 28.	6.1	More Details
CVE-2023-40983	A reflected cross-site scripting (XSS) vulnerability in the File Manager function of Webmin v2.100 allows attackers to execute malicious scripts via injecting a crafted payload into the Find in Results file.	6.1	More Details
CVE-2023-29305	Adobe Connect versions 12.3 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	6.1	More Details
CVE-2023-4985	A vulnerability classified as critical has been found in Supcon InPlant SCADA up to 20230901. Affected is an unknown function of the file Project.xml. The manipulation leads to improper authentication. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-239796. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.9	More Details
CVE-2023-32182	A Improper Link Resolution Before File Access ('Link Following') vulnerability in SUSE SUSE Linux Enterprise Desktop 15 SP5 postfix, SUSE SUSE Linux Enterprise High Performance Computing 15 SP5 postfix, SUSE openSUSE Leap 15.5 postfix.This issue affects SUSE Linux Enterprise Desktop 15 SP5: before 3.7.3-150500.3.5.1; SUSE Linux Enterprise High Performance Computing 15 SP5: before 3.7.3-150500.3.5.1; openSUSE Leap 15.5 : before 3.7.3-150500.3.5.1.	5.9	More Details
CVE-2023-4806	A flaw was found in glibc. In an extremely rare situation, the getaddrinfo function may access memory that has been freed, resulting in an application crash. This issue is only exploitable when a NSS module implements only the _nss_*_gethostbyname2_r and _nss_*_getcanonname_r hooks without implementing the _nss_*_gethostbyname3_r hook. The resolved name should return a large number of IPv6 and IPv4, and the call to the getaddrinfo function should have the AF_INET6 address family with AI_CANONNAME, AI_ALL and AI_V4MAPPED as flags.	5.9	More Details
CVE-2023-38353	MiniTool Power Data Recovery version 11.6 and before contains an insecure in-app payment system that allows attackers to steal highly sensitive information through a man in the middle attack.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5054	The Super Store Finder plugin for WordPress is vulnerable to unauthenticated arbitrary email creation and relay in versions up to, and including, 6.9.3. This is due to insufficient restrictions on the sendMail.php file that allows direct access. This makes it possible for unauthenticated attackers to send emails utilizing the vulnerable site's server, with arbitrary content. Please note that this vulnerability has already been publicly disclosed with an exploit which is why we are publishing the details without a patch available, we are attempting to initiate contact with the developer.	5.8	More Details
CVE-2023-36472	Strapi is an open-source headless content management system. Prior to version 4.11.7, an unauthorized actor can get access to user reset password tokens if they have the configure view permissions. The `/content-manager/relations` route does not remove private fields or ensure that they can't be selected. This issue is fixed in version 4.11.7.	5.8	More Details
CVE-2023-20191	A vulnerability in the access control list (ACL) processing on MPLS interfaces in the ingress direction of Cisco IOS XR Software could allow an unauthenticated, remote attacker to bypass a configured ACL. This vulnerability is due to incomplete support for this feature. An attacker could exploit this vulnerability by attempting to send traffic through an affected device. A successful exploit could allow the attacker to bypass an ACL on the affected device. There are workarounds that address this vulnerability. This advisory is part of the September 2023 release of the Cisco IOS XR Software Security Advisory Bundled Publication. For a complete list of the advisories and links to them, see Cisco Event Response: September 2023 Semiannual Cisco IOS XR Software Security Advisory Bundled Publication .	5.8	More Details
CVE-2023-20190	A vulnerability in the classic access control list (ACL) compression feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to bypass the protection that is offered by a configured ACL on an affected device. This vulnerability is due to incorrect destination address range encoding in the compression module of an ACL that is applied to an interface of an affected device. An attacker could exploit this vulnerability by sending traffic through the affected device that should be denied by the configured ACL. A successful exploit could allow the attacker to bypass configured ACL protections on the affected device, allowing the attacker to access trusted networks that the device might be protecting. There are workarounds that address this vulnerability. This advisory is part of the September 2023 release of the Cisco IOS XR Software Security Advisory Bundled Publication. For a complete list of the advisories and links to them, see Cisco Event Response: September 2023 Semiannual Cisco IOS XR Software Security Advisory Bundled Publication .	5.8	More Details
CVE-2023-20135	A vulnerability in Cisco IOS XR Software image verification checks could allow an authenticated, local attacker to execute arbitrary code on the underlying operating system. This vulnerability is due to a time-of-check, time-of-use (TOCTOU) race condition when an install query regarding an ISO image is performed during an install operation that uses an ISO image. An attacker could exploit this vulnerability by modifying an ISO image and then carrying out install requests in parallel. A successful exploit could allow the attacker to execute arbitrary code on an affected device.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3892	Improper Restriction of XML External Entity Reference vulnerability in MIM Assistant and Client DICOM RTst Loading modules allows XML Entity Linking / XML External Entities Blowup. In order to take advantage of this vulnerability, an attacker must craft a malicious XML document, embed this document into specific 3rd party private RTst metadata tags, transfer the now compromised DICOM object to MIM, and force MIM to archive and load the data. Users on either version are strongly encouraged to update to an unaffected version (7.2.11+, 7.3.4+). This issue was found and analyzed by MIM Software's internal security team. We are unaware of any proof of concept or actual exploit available in the wild. For more information, visit https://www.mimsoftware.com/cve-2023-3892 https://www.mimsoftware.com/cve-2023-3892 This issue affects MIM Assistant: 7.2.10, 7.3.3; MIM Client: 7.2.10, 7.3.3.	5.6	More Details
CVE-2023-3301	A flaw was found in QEMU. The async nature of hot-unplug enables a race scenario where the net device backend is cleared before the virtio-net pci frontend has been unplugged. A malicious guest could use this time window to trigger an assertion and cause a denial of service.	5.6	More Details
CVE-2023-5029	A vulnerability, which was classified as critical, was found in mccms 2.6. This affects an unknown part of the file /category/order/hits/copyright/46/finish/1/list/1. The manipulation with the input "'1 leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-239871.	5.5	More Details
CVE-2023-38558	A vulnerability has been identified in SIMATIC PCS neo (Administration Console) V4.0 (All versions), SIMATIC PCS neo (Administration Console) V4.0 Update 1 (All versions). The affected application leaks Windows admin credentials. An attacker with local access to the Administration Console could get the credentials, and impersonate the admin user, thereby gaining admin access to other Windows systems.	5.5	More Details
CVE-2023-4987	A vulnerability, which was classified as critical, has been found in infinitietech taskhub 2.8.7. Affected by this issue is some unknown functionality of the file /home/get_tasks_list of the component GET Parameter Handler. The manipulation of the argument project/status/user_id/sort/search leads to sql injection. VDB-239798 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-41010	Insecure Permissions vulnerability in Sichuan Tianyi Kanghe Communication Co., Ltd China Telecom Tianyi Home Gateway v.TEWA-700G allows a local attacker to obtain sensitive information via the default password parameter.	5.5	More Details
CVE-2023-36160	An issue was discovered in Qubo Smart Plug10A version HSP02_01_01_14_SYSTEM-10 A, allows local attackers to gain sensitive information and other unspecified impact via UART console.	5.5	More Details
CVE-2023-5022	A vulnerability has been found in DedeCMS up to 5.7.100 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /include/dialog/select_templets_post.php. The manipulation of the argument activepath leads to absolute path traversal. The associated identifier of this vulnerability is VDB-239863.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42503	Improper Input Validation, Uncontrolled Resource Consumption vulnerability in Apache Commons Compress in TAR parsing.This issue affects Apache Commons Compress: from 1.22 before 1.24.0. Users are recommended to upgrade to version 1.24.0, which fixes the issue. A third party can create a malformed TAR file by manipulating file modification times headers, which when parsed with Apache Commons Compress, will cause a denial of service issue via CPU consumption. In version 1.22 of Apache Commons Compress, support was added for file modification times with higher precision (issue # COMPRESS-612 [1]). The format for the PAX extended headers carrying this data consists of two numbers separated by a period [2], indicating seconds and subsecond precision (for example “1647221103.5998539”). The impacted fields are “atime”, “ctime”, “mtime” and “LIBARCHIVE.creationtime”. No input validation is performed prior to the parsing of header values. Parsing of these numbers uses the BigDecimal [3] class from the JDK which has a publicly known algorithmic complexity issue when doing operations on large numbers, causing denial of service (see issue # JDK-6560193 [4]). A third party can manipulate file time headers in a TAR file by placing a number with a very long fraction (300,000 digits) or a number with exponent notation (such as “9e9999999”) within a file modification time header, and the parsing of files with these headers will take hours instead of seconds, leading to a denial of service via exhaustion of CPU resources. This issue is similar to CVE-2012-2098 [5]. [1]: https://issues.apache.org/jira/browse/COMPRESS-612 [2]: https://pubs.opengroup.org/onlinepubs/9699919799/utilities/pax.html#tag_20_92_13_05 [3]: https://docs.oracle.com/javase/8/docs/api/java/math/BigDecimal.html [4]: https://bugs.openjdk.org/browse/JDK-6560193 [5]: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2098 Only applications using CompressorStreamFactory class (with auto-detection of file types), TarArchiveInputStream and TarFile classes to parse TAR files are impacted. Since this code was introduced in v1.22, only that version and later versions are impacted.	5.5	More Details
CVE-2023-5023	A vulnerability was found in Tongda OA 2017 and classified as critical. Affected by this issue is some unknown functionality of the file general/hr/manage/staff_relatives/delete.php. The manipulation of the argument RELATIVES_ID leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-239864.	5.5	More Details
CVE-2023-5030	A vulnerability has been found in Tongda OA up to 11.10 and classified as critical. This vulnerability affects unknown code of the file general/hr/recruit/plan/delete.php. The manipulation of the argument PLAN_ID leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-239872.	5.5	More Details
CVE-2023-5017	A vulnerability was found in lmxcms up to 1.41. It has been rated as critical. Affected by this issue is some unknown functionality of the file admin.php. The manipulation of the argument lid leads to sql injection. VDB-239858 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-43114	An issue was discovered in Qt before 5.15.16, 6.x before 6.2.10, and 6.3.x through 6.5.x before 6.5.3 on Windows. When using the GDI font engine, if a corrupted font is loaded via QFontDatabase::addApplicationFont{FromData], then it can cause the application to crash because of missing length checks.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3280	A problem with a protection mechanism in the Palo Alto Networks Cortex XDR agent on Windows devices allows a local user to disable the agent.	5.5	More Details
CVE-2023-40715	A cleartext storage of sensitive information vulnerability [CWE-312] in FortiTester 2.3.0 through 7.2.3 may allow an attacker with access to the DB contents to retrieve the plaintext password of external servers configured in the device.	5.5	More Details
CVE-2023-4093	Reflected and persistent XSS vulnerability in Arconte Áurea, in its 1.5.0.0 version. The exploitation of this vulnerability could allow an attacker to inject malicious JavaScript code, compromise the victim's browser and take control of it, redirect the user to malicious domains or access information being viewed by the legitimate user.	5.5	More Details
CVE-2023-29499	A flaw was found in GLib. GVariant deserialization fails to validate that the input conforms to the expected format, leading to denial of service.	5.5	More Details
CVE-2023-25608	An incomplete filtering of one or more instances of special elements vulnerability [CWE-792] in the command line interpreter of FortiAP-W2 7.2.0 through 7.2.1, 7.0.3 through 7.0.5, 7.0.0 through 7.0.1, 6.4 all versions, 6.2 all versions, 6.0 all versions; FortiAP-C 5.4.0 through 5.4.4, 5.2 all versions; FortiAP 7.2.0 through 7.2.1, 7.0.0 through 7.0.5, 6.4 all versions, 6.0 all versions; FortiAP-U 7.0.0, 6.2.0 through 6.2.5, 6.0 all versions, 5.4 all versions may allow an authenticated attacker to read arbitrary files via specially crafted command arguments.	5.5	More Details
CVE-2023-32611	A flaw was found in GLib. GVariant deserialization is vulnerable to a slowdown issue where a crafted GVariant can cause excessive processing, leading to denial of service.	5.5	More Details
CVE-2023-32665	A flaw was found in GLib. GVariant deserialization is vulnerable to an exponential blowup issue where a crafted GVariant can cause excessive processing, leading to denial of service.	5.5	More Details
CVE-2023-40986	A stored cross-site scripting (XSS) vulnerability in the Usermin Configuration function of Webmin v2.100 allows attackers to execute arbitrary web sripts or HTML via a crafted payload injected into the Custom field.	5.4	More Details
CVE-2023-41436	Cross Site Scripting vulnerability in CSZCMS v.1.3.0 allows a local attacker to execute arbitrary code via a crafted script to the Additional Meta Tag parameter in the Pages Content Menu component.	5.4	More Details
CVE-2023-38215	Adobe Experience Manager versions 6.5.17 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2023-23957	An authenticated user can see and modify the value for ‘next’ query parameter in Symantec Identity Portal 14.4	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38214	Adobe Experience Manager versions 6.5.17 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2023-40984	A reflected cross-site scripting (XSS) vulnerability in the File Manager function of Webmin v2.100 allows attackers to execute malicious scripts via injecting a crafted payload into the Replace in Results file.	5.4	More Details
CVE-2023-40985	An issue was discovered in Webmin 2.100. The File Manager functionality allows an attacker to exploit a Cross-Site Scripting (XSS) vulnerability. By providing a malicious payload, an attacker can inject arbitrary code, which is then executed within the context of the victim's browser when any file is searched/replaced.	5.4	More Details
CVE-2023-41158	A Stored Cross-Site Scripting (XSS) vulnerability in the MIME type programs tab in Usermin 2.000 allows remote attackers to inject arbitrary web script or HTML via the description field while creating a new MIME type program.	5.4	More Details
CVE-2023-4977	Code Injection in GitHub repository librenms/librenms prior to 23.9.0.	5.4	More Details
CVE-2023-41157	Multiple stored cross-site scripting (XSS) vulnerabilities in Usermin 2.000 allow remote attackers to inject arbitrary web script or HTML via the folder name parameter while creating the folder to manage the folder tab, filter tab, and forward mail tab.	5.4	More Details
CVE-2023-4979	Cross-site Scripting (XSS) - Reflected in GitHub repository librenms/librenms prior to 23.9.0.	5.4	More Details
CVE-2023-4980	Cross-site Scripting (XSS) - Generic in GitHub repository librenms/librenms prior to 23.9.0.	5.4	More Details
CVE-2023-4981	Cross-site Scripting (XSS) - DOM in GitHub repository librenms/librenms prior to 23.9.0.	5.4	More Details
CVE-2023-42450	Mastodon is a free, open-source social network server based on ActivityPub. Starting in version 4.2.0-beta1 and prior to version 4.2.0-rc2, by crafting specific input, attackers can inject arbitrary data into HTTP requests issued by Mastodon. This can be used to perform confused deputy attacks if the server configuration includes `ALLOWED_PRIVATE_ADDRESSES` to allow access to local exploitable services. Version 4.2.0-rc2 has a patch for the issue.	5.4	More Details
CVE-2023-4982	Cross-site Scripting (XSS) - Stored in GitHub repository librenms/librenms prior to 23.9.0.	5.4	More Details
CVE-2023-40982	A stored cross-site scripting (XSS) vulnerability in Webmin v2.100 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the cloned module name parameter.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40932	A Cross-site scripting (XSS) vulnerability in Nagios XI version 5.11.1 and below allows authenticated attackers with access to the custom logo component to inject arbitrary javascript or HTML via the alt-text field. This affects all pages containing the navbar including the login page which means the attacker is able to to steal plaintext credentials.	5.4	More Details
CVE-2023-39777	A cross-site scripting (XSS) vulnerability in the Admin Control Panel of vBulletin 5.7.5 and 6.0.0 allows attackers to execute arbitrary web scripts or HTML via the /login.php?do=login url parameter.	5.4	More Details
CVE-2023-41592	Froala Editor v4.0.1 to v4.1.1 was discovered to contain a cross-site scripting (XSS) vulnerability.	5.4	More Details
CVE-2023-42371	Cross Site Scripting vulnerability in Summernote Rich Text Editor v.0.8.18 and before allows a remote attacker to execute arbitrary code via a crafted script to the insert link function in the editor component.	5.4	More Details
CVE-2023-37611	Cross Site Scripting (XSS) vulnerability in Neos CMS 8.3.3 allows a remote authenticated attacker to execute arbitrary code via a crafted SVG file to the neos/management/media component.	5.4	More Details
CVE-2023-41156	A Stored Cross-Site Scripting (XSS) vulnerability in the filter and forward mail tab in Usermin 2.001 allows remote attackers to inject arbitrary web script or HTML via the save to new folder named field while creating a new filter.	5.4	More Details
CVE-2023-41160	A Stored Cross-Site Scripting (XSS) vulnerability in the SSH configuration tab in Usermin 2.001 allows remote attackers to inject arbitrary web script or HTML via the key name field while adding an authorized key.	5.4	More Details
CVE-2023-41155	A Stored Cross-Site Scripting (XSS) vulnerability in the mail forwarding and replies tab in Webmin and Usermin 2.000 allows remote attackers to inject arbitrary web script or HTML via the forward to field while creating a mail forwarding rule.	5.4	More Details
CVE-2023-41159	A Stored Cross-Site Scripting (XSS) vulnerability while editing the autoreply file page in Usermin 2.000 allows remote attackers to inject arbitrary web script or HTML by editing the forward file manually.	5.4	More Details
CVE-2023-41154	A Stored Cross-Site Scripting (XSS) vulnerability in the scheduled cron jobs tab in Usermin 2.000 allows remote attackers to inject arbitrary web script or HTML via the value field parameter while creating a new environment variable.	5.4	More Details
CVE-2023-42362	An arbitrary file upload vulnerability in Teller Web App v.4.4.0 allows a remote attacker to execute arbitrary commands and obtain sensitive information via uploading a crafted file.	5.4	More Details
CVE-2023-41152	A Stored Cross-Site Scripting (XSS) vulnerability in the MIME type programs tab in Usermin 2.000 allows remote attackers to inject arbitrary web script or HTML via the handle program field while creating a new MIME type program.	5.4	More Details
CVE-2023-3588	A stored Cross-site Scripting (XSS) vulnerability affecting Teamwork Cloud from No Magic Release 2021x through No Magic Release 2022x allows an attacker to execute arbitrary script code.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37459	Contiki-NG is an operating system for internet-of-things devices. In versions 4.9 and prior, when a packet is received, the Contiki-NG network stack attempts to start the periodic TCP timer if it is a TCP packet with the SYN flag set. But the implementation does not first verify that a full TCP header has been received. Specifically, the implementation attempts to access the flags field from the TCP buffer in the following conditional expression in the `check_for_tcp_syn` function. For this reason, an attacker can inject a truncated TCP packet, which will lead to an out-of-bound read from the packet buffer. As of time of publication, a patched version is not available. As a workaround, one can apply the changes in Contiki-NG pull request #2510 to patch the system.	5.3	More Details
CVE-2023-32643	A flaw was found in GLib. The GVariant deserialization code is vulnerable to a heap buffer overflow introduced by the fix for CVE-2023-32665. This bug does not affect any released version of GLib, but does affect GLib distributors who followed the guidance of GLib developers to backport the initial fix for CVE-2023-32665.	5.3	More Details
CVE-2023-37281	Contiki-NG is an operating system for internet-of-things devices. In versions 4.9 and prior, when processing the various IPv6 header fields during IPHC header decompression, Contiki-NG confirms the received packet buffer contains enough data as needed for that field. But no similar check is done before decompressing the IPv6 address. Therefore, up to 16 bytes can be read out of bounds on the line with the statement `memcpy(&ipaddr->u8[16 - postcount], iphc_ptr, postcount);`. The value of `postcount` depends on the address compression used in the received packet and can be controlled by the attacker. As a result, an attacker can inject a packet that causes an out-of-bound read. As of time of publication, a patched version is not available. As a workaround, one can apply the changes in Contiki-NG pull request #2509 to patch the system.	5.3	More Details
CVE-2023-42468	The com.cutestudio.colordialer application through 2.1.8-2 for Android allows a remote attacker to initiate phone calls without user consent, because of improper export of the com.cutestudio.dialer.activities.DialerActivity component. A third-party application (without any permissions) can craft an intent targeting com.cutestudio.dialer.activities.DialerActivity via the android.intent.action.CALL action in conjunction with a tel: URI, thereby placing a phone call.	5.3	More Details
CVE-2023-4155	A flaw was found in KVM AMD Secure Encrypted Virtualization (SEV) in the Linux kernel. A KVM guest using SEV-ES or SEV-SNP with multiple vCPUs can trigger a double fetch race condition vulnerability and invoke the `VMGEXIT` handler recursively. If an attacker manages to call the handler multiple times, they can trigger a stack overflow and cause a denial of service or potentially guest-to-host escape in kernel configurations without stack guard pages (`CONFIG_VMAP_STACK`).	5.3	More Details
CVE-2023-4917	The Leyka plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 3.30.3 via the 'leyka_ajax_get_env_and_options' function. This can allow authenticated attackers with subscriber-level permissions or above to extract sensitive data including Sberbank API key and password, PayPal Client Secret, and more keys and passwords.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4915	The WP User Control plugin for WordPress is vulnerable to unauthorized password resets in versions up to, and including 1.5.3. This is due to the plugin using native password reset functionality, with insufficient validation on the password reset function (in the WP User Control Widget). The function changes the user's password after providing the email. The new password is only sent to the user's email, so the attacker does not have access to the new password.	5.3	More Details
CVE-2023-27998	A lack of custom error pages vulnerability [CWE-756] in FortiPresence versions 1.2.0 through 1.2.1 and all versions of 1.1 and 1.0 may allow an unauthenticated attacker with the ability to navigate to the login GUI to gain sensitive information via navigating to specific HTTP(s) paths.	5.3	More Details
CVE-2023-40167	Jetty is a Java based web server and servlet engine. Prior to versions 9.4.52, 10.0.16, 11.0.16, and 12.0.1, Jetty accepts the `+` character proceeding the content-length value in a HTTP/1 header field. This is more permissive than allowed by the RFC and other servers routinely reject such requests with 400 responses. There is no known exploit scenario, but it is conceivable that request smuggling could result if jetty is used in combination with a server that does not close the connection after sending such a 400 response. Versions 9.4.52, 10.0.16, 11.0.16, and 12.0.1 contain a patch for this issue. There is no workaround as there is no known exploit scenario.	5.3	More Details
CVE-2023-38206	Adobe ColdFusion versions 2018u18 (and earlier), 2021u8 (and earlier) and 2023u2 (and earlier) are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to access the administration CFM and CFC endpoints resulting in a low-confidentiality impact. Exploitation of this issue does not require user interaction.	5.3	More Details
CVE-2023-40788	SpringBlade <=V3.6.0 is vulnerable to Incorrect Access Control due to incorrect configuration in the default gateway resulting in unauthorized access to error logs	5.3	More Details
CVE-2023-5012	A vulnerability, which was classified as problematic, was found in Topaz OFD 2.11.0.201. This affects an unknown part of the file C:\Program Files\Topaz OFD\Warsaw\core.exe of the component Protection Module Warsaw. The manipulation leads to unquoted search path. Attacking locally is a requirement. Upgrading to version 2.12.0.259 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-239853 was assigned to this vulnerability.	5.3	More Details
CVE-2023-40717	A use of hard-coded credentials vulnerability [CWE-798] in FortiTester 2.3.0 through 7.2.3 may allow an attacker who managed to get a shell on the device to access the database via shell commands.	5.3	More Details
CVE-2023-41599	An issue in the component /common/DownController.java of JFinalCMS v5.0.0 allows attackers to execute a directory traversal.	5.3	More Details
CVE-2023-4095	User enumeration vulnerability in Arconte Áurea 1.5.0.0 version. The exploitation of this vulnerability could allow an attacker to obtain a list of registered users in the application, obtaining the necessary information to perform more complex attacks on the platform.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42441	Vyper is a Pythonic Smart Contract Language for the Ethereum Virtual Machine (EVM). Starting in version 0.2.9 and prior to version 0.3.10, locks of the type `@nonreentrant("")` or `@nonreentrant('')` do not produce reentrancy checks at runtime. This issue is fixed in version 0.3.10. As a workaround, ensure the lock name is a non-empty string.	5.3	More Details
CVE-2023-41889	SHIRASAGI is a Content Management System. Prior to version 1.18.0, SHIRASAGI is vulnerable to a Post-Unicode normalization issue. This happens when a logical validation or a security check is performed before a Unicode normalization. The Unicode character equivalent of a character would resurface after the normalization. The fix is initially performing the Unicode normalization and then strip for all whitespaces and then checking for a blank string. This issue has been fixed in version 1.18.0.	5.3	More Details
CVE-2023-32461	Dell PowerEdge BIOS and Dell Precision BIOS contain a buffer overflow vulnerability. A local malicious user with high privileges could potentially exploit this vulnerability, leading to corrupt memory and potentially escalate privileges.	5.0	More Details
CVE-2023-41042	Discourse is an open-source discussion platform. Prior to version 3.1.1 of the `stable` branch and version 3.2.0.beta1 of the `beta` and `tests-passed` branches, importing a remote theme loads their assets into memory without enforcing limits for file size or number of files. The issue is patched in version 3.1.1 of the `stable` branch and version 3.2.0.beta1 of the `beta` and `tests-passed` branches. There are no known workarounds.	4.9	More Details
CVE-2023-4039	**DISPUTED**A failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer overflow in dynamically-sized local variables in your application without this being detected. This stack-protector failure only applies to C99-style dynamically-sized local variables or those created using alloca(). The stack-protector operates as intended for statically-sized local variables. The default behavior when the stack-protector detects an overflow is to terminate your application, resulting in controlled loss of availability. An attacker who can exploit a buffer overflow without triggering the stack-protector might be able to change program flow control to cause an uncontrolled loss of availability or to go further and affect confidentiality or integrity. NOTE: The GCC project argues that this is a missed hardening bug and not a vulnerability by itself.	4.8	More Details
CVE-2023-4803	A reflected cross-site scripting vulnerability in the WriteWindowTitle endpoint of the Insider Threat Management (ITM) Server's web console could be used by an authenticated administrator to run arbitrary javascript within another web console administrator's browser. All versions prior to 7.14.3.69 are affected.	4.8	More Details
CVE-2023-2995	The Leyka WordPress plugin before 3.30.4 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-2023-4376	The Serial Codes Generator and Validator with WooCommerce Support WordPress plugin before 2.4.15 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-2023-4802	A reflected cross-site scripting vulnerability in the UpdateInstalledSoftware endpoint of the Insider Threat Management (ITM) Server's web console could be used by an authenticated administrator to run arbitrary javascript within another web console administrator's browser. All versions prior to 7.14.3.69 are affected.	4.8	More Details
CVE-2022-3466	The version of cri-o as released for Red Hat OpenShift Container Platform 4.9.48, 4.10.31, and 4.11.6 via RHBA-2022:6316, RHBA-2022:6257, and RHBA-2022:6658, respectively, included an incorrect version of cri-o missing the fix for CVE-2022-27652, which was previously fixed in OCP 4.9.41 and 4.10.12 via RHBA-2022:5433 and RHSA-2022:1600. This issue could allow an attacker with access to programs with inheritable file capabilities to elevate those capabilities to the permitted set when execve(2) runs. For more details, see https://access.redhat.com/security/cve/CVE-2022-27652.	4.8	More Details
CVE-2023-41626	Gradio v3.27.0 was discovered to contain an arbitrary file upload vulnerability via the /upload interface.	4.8	More Details
CVE-2023-25585	A flaw was found in Binutils. The use of an uninitialized field in the struct module *module may lead to application crash and local denial of service.	4.7	More Details
CVE-2023-32636	A flaw was found in glib, where the gvariant deserialization code is vulnerable to a denial of service introduced by additional input validation added to resolve CVE-2023-29499. The offset table validation may be very slow. This bug does not affect any released version of glib but does affect glib distributors who followed the guidance of glib developers to backport the initial fix for CVE-2023-29499.	4.7	More Details
CVE-2023-25586	A flaw was found in Binutils. A logic fail in the bfd_init_section_decompress_status function may lead to the use of an uninitialized variable that can cause a crash and local denial of service.	4.7	More Details
CVE-2023-25588	A flaw was found in Binutils. The field `the_bfd` of `asymbol`struct is uninitialized in the `bfd_mach_o_get_synthetic_symtab` function, which may lead to an application crash and local denial of service.	4.7	More Details
CVE-2022-3261	A flaw was found in OpenStack. Multiple components show plain-text passwords in /var/log/messages during the OpenStack overcloud update run, leading to a disclosure of sensitive information problem.	4.4	More Details
CVE-2022-20917	A vulnerability in the Extensible Messaging and Presence Protocol (XMPP) message processing feature of Cisco Jabber could allow an authenticated, remote attacker to manipulate the content of XMPP messages that are used by the affected application. This vulnerability is due to the improper handling of nested XMPP messages within requests that are sent to the Cisco Jabber client software. An attacker could exploit this vulnerability by connecting to an XMPP messaging server and sending crafted XMPP messages to an affected Jabber client. A successful exploit could allow the attacker to manipulate the content of XMPP messages, possibly allowing the attacker to cause the Jabber client application to perform unsafe actions.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39285	A vulnerability in the Edge Gateway component of Mitel MiVoice Connect through 19.3 SP3 (22.24.5800.0) could allow an unauthenticated attacker to perform a Cross Site Request Forgery (CSRF) attack due to insufficient request validation. A successful exploit could allow an attacker to provide a modified URL, potentially enabling them to modify system configuration settings.	4.3	More Details
CVE-2023-39286	A vulnerability in the Connect Mobility Router component of Mitel MiVoice Connect through 9.6.2304.102 could allow an unauthenticated attacker to perform a Cross Site Request Forgery (CSRF) attack due to insufficient request validation. A successful exploit could allow an attacker to provide a modified URL, potentially enabling them to modify system configuration settings.	4.3	More Details
CVE-2021-28485	In Ericsson Mobile Switching Center Server (MSC-S) before IS 3.1 CP22, the SIS web application allows relative path traversal via a specific parameter in the https request after authentication, which allows access to files on the system that are not intended to be accessible via the web application.	4.3	More Details
CVE-2023-20233	A vulnerability in the Connectivity Fault Management (CFM) feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to incorrect processing of invalid continuity check messages (CCMs). An attacker could exploit this vulnerability by sending crafted CCMs to an affected device. A successful exploit could allow the attacker to cause the CFM service to crash when a user displays information about maintenance end points (MEPs) for peer MEPs on an affected device.	4.3	More Details
CVE-2023-4983	A vulnerability was found in app1pro Shopicial up to 20230830. It has been declared as problematic. This vulnerability affects unknown code of the file search. The manipulation of the argument from with the input comments</script>"><img src=x onerror=alert(document.cookie)> leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-239794 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2021-44172	An exposure of sensitive information to an unauthorized actor vulnerability [CWE-200] in FortiClientEMS versions 7.0.0 through 7.0.4, 7.0.6 through 7.0.7, in all 6.4 and 6.2 version management interface may allow an unauthenticated attacker to gain information on environment variables such as the EMS installation path.	4.3	More Details
CVE-2023-4984	A vulnerability was found in didi KnowSearch 0.3.2/0.3.1.2. It has been rated as problematic. This issue affects some unknown processing of the file /api/es/admin/v3/security/user/1. The manipulation leads to unprotected storage of credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-239795.	4.3	More Details
CVE-2023-4948	The WooCommerce CVR Payment Gateway plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the refresh_order_cvr_data AJAX action in versions up to 6.1.0. This makes it possible for authenticated attackers with contributor-level access and above, to update CVR numbers for orders.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36551	A exposure of sensitive information to an unauthorized actor in Fortinet FortiSIEM version 6.7.0 through 6.7.5 allows attacker to information disclosure via a crafted http request.	4.3	More Details
CVE-2023-36638	An improper privilege management vulnerability [CWE-269] in FortiManager 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions and FortiAnalyzer 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions API may allow a remote and authenticated API admin user to access some system settings such as the mail server settings through the API via a stolen GUI session ID.	4.3	More Details
CVE-2023-4973	A vulnerability was found in Academy LMS 6.2 on Windows. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /academy/tutor/filter of the component GET Parameter Handler. The manipulation of the argument searched_word/searched_tution_class_type[]/searched_price_type[]/searched_duration[] leads to cross site scripting. The attack can be launched remotely. The identifier VDB-239749 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-5026	A vulnerability classified as problematic has been found in Tongda OA 11.10. Affected is an unknown function of the file /general/ipanel/menu_code.php?MENU_TYPE=FAV. The manipulation of the argument OA_SUB_WINDOW leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-239868.	3.5	More Details
CVE-2023-36479	Eclipse Jetty Canonical Repository is the canonical repository for the Jetty project. Users of the CgiServlet with a very specific command structure may have the wrong command executed. If a user sends a request to a org.eclipse.jetty.servlets.CGI Servlet for a binary with a space in its name, the servlet will escape the command by wrapping it in quotation marks. This wrapped command, plus an optional command prefix, will then be executed through a call to Runtime.exec. If the original binary name provided by the user contains a quotation mark followed by a space, the resulting command line will contain multiple tokens instead of one. This issue was patched in version 9.4.52, 10.0.16, 11.0.16 and 12.0.0-beta2.	3.5	More Details
CVE-2023-5024	A vulnerability was found in Planno 23.04.04. It has been classified as problematic. This affects an unknown part of the component Comment Handler. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-239865 was assigned to this vulnerability.	3.5	More Details
CVE-2023-5025	A vulnerability was found in KOHA up to 23.05.03. It has been declared as problematic. This vulnerability affects unknown code of the file /cgi-bin/koha/catalogue/search.pl of the component MARC. The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-239866 is the identifier assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5021	A vulnerability, which was classified as problematic, was found in SourceCodester AC Repair and Services System 1.0. Affected is an unknown function of the file admin/?page=system_info/contact_information. The manipulation of the argument telephone/mobile/address leads to cross site scripting. It is possible to launch the attack remotely. VDB-239862 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-43566	In JetBrains TeamCity before 2023.05.4 stored XSS was possible during nodes configuration	3.5	More Details
CVE-2023-5015	A vulnerability was found in UCMS 1.4.7. It has been classified as problematic. Affected is an unknown function of the file ajax.php?do=strarraylist. The manipulation of the argument strdefault leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-239856.	3.5	More Details
CVE-2023-41900	Jetty is a Java based web server and servlet engine. Versions 9.4.21 through 9.4.51, 10.0.15, and 11.0.15 are vulnerable to weak authentication. If a Jetty `OpenIdAuthenticator` uses the optional nested `LoginService`, and that `LoginService` decides to revoke an already authenticated user, then the current request will still treat the user as authenticated. The authentication is then cleared from the session and subsequent requests will not be treated as authenticated. So a request on a previously authenticated session could be allowed to bypass authentication after it had been rejected by the `LoginService`. This impacts usages of the jetty-openid which have configured a nested `LoginService` and where that `LoginService` will is capable of rejecting previously authenticated users. Versions 9.4.52, 10.0.16, and 11.0.16 have a patch for this issue.	3.5	More Details
CVE-2023-42469	The com.full.dialer.top.secure.encrypted application through 1.0.1 for Android enables any installed application (with no permissions) to place phone calls without user interaction by sending a crafted intent via the com.full.dialer.top.secure.encrypted.activities.DialerActivity component.	3.3	More Details
CVE-2020-36766	An issue was discovered in the Linux kernel before 5.8.6. drivers/media/cec/core/cec-api.c leaks one byte of kernel memory on specific hardware to unprivileged users, because of directly assigning log_addrs with a hole in the struct.	3.3	More Details
CVE-2023-4965	A vulnerability was found in phpipam 1.5.1. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Header Handler. The manipulation of the argument X-Forwarded-Host leads to open redirect. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-239732.	2.7	More Details
CVE-2023-5013	A vulnerability has been found in Pluck CMS 4.7.18 and classified as problematic. This vulnerability affects unknown code of the file install.php of the component Installation Handler. The manipulation of the argument contents with the input <script>alert('xss')</script> leads to cross site scripting. The attack can be initiated 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. VDB-239854 is the identifier assigned to this vulnerability.	2.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4986	A vulnerability classified as problematic was found in Supcon InPlant SCADA up to 20230901. Affected by this vulnerability is an unknown functionality of the file Project.xml. The manipulation leads to password hash with insufficient computational effort. Local access is required to approach this attack. 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 VDB-239797 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.5	More Details
CVE-2023-41880	Wasmtime is a standalone runtime for WebAssembly. Wasmtime versions from 10.0.0 to versions 10.02, 11.0.2, and 12.0.1 contain a miscompilation of the WebAssembly `i64x2.shr_s` instruction on x86_64 platforms when the shift amount is a constant value that is larger than 32. Only x86_64 is affected so all other targets are not affected by this. The miscompilation results in the instruction producing an incorrect result, namely the low 32-bits of the second lane of the vector are derived from the low 32-bits of the second lane of the input vector instead of the high 32-bits. The primary impact of this issue is that any WebAssembly program using the `i64x2.shr_s` with a constant shift amount larger than 32 may produce an incorrect result. This issue is not an escape from the WebAssembly sandbox. Execution of WebAssembly guest programs will still behave correctly with respect to memory sandboxing and isolation from the host. Wasmtime considers non-spec-compliant behavior as a security issue nonetheless. This issue was discovered through fuzzing of Wasmtime's code generator Cranelift. Wasmtime versions 10.0.2, 11.0.2, and 12.0.2 are all patched to no longer have this miscompilation. This issue only affects x86_64 hosts and the only workaround is to either scan for this pattern in wasm modules which is nontrivial or to disable the SIMD proposal for WebAssembly. Users prior to 10.0.0 are unaffected by this vulnerability.	2.2	More Details
CVE-2023-5028	A vulnerability, which was classified as problematic, has been found in China Unicom TEWA-800G 4.16L.04_CT2015_Yueme. Affected by this issue is some unknown functionality. The manipulation leads to information exposure through debug log file. It is possible to launch the attack on the physical device. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. VDB-239870 is the identifier assigned to this vulnerability.	2.0	More Details
CVE-2023-4951	A cross site scripting issue was discovered with the pagination function on the "Client-based Authentication Policy Configuration" screen of the GreenRADIUS web admin interface. This issue is found in GreenRADIUS v5.1.1.1 and prior. A fix was included in v5.1.2.2.	2.0	More Details
CVE-2018-4750	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4749	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4751	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4752	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4753	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4772	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4748	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4737	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4728	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4729	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4730	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4731	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4732	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4733	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4734	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4735	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4736	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4738	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4747	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4739	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4740	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4741	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4742	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4743	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4744	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4745	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4755	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4746	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4754	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4760	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4756	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4782	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4774	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4771	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4770	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4769	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4775	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4768	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4776	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4777	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4778	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4779	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4780	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4781	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4783	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4757	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4767	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4766	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4765	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4764	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4763	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4726	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4762	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4761	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4773	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4784	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4759	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4758	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4727	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4676	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4725	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4680	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4692	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4691	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4690	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4689	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4688	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4687	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4686	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4685	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4684	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4683	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4682	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4681	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4679	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4694	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4678	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4677	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4786	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4675	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4674	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4673	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4672	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4671	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4670	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4669	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4668	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4667	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4693	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4695	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4724	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4711	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4723	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4722	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4721	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4720	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4719	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4718	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4717	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4716	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4715	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4714	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4713	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4712	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4710	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4696	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4709	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4708	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4707	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4706	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4705	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4704	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4703	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4702	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4701	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4699	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4698	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4697	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4785	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2010-1835	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4787	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8882	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8894	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8893	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8892	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8891	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8890	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8889	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8888	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8887	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8886	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8885	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8884	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-8883	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8881	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8896	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8880	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8879	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8878	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8877	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8876	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8875	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8874	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8873	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8872	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8871	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-8870	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8869	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8895	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8897	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8867	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2009-3773	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2023-4701	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority as the vendor eventually states that this issue is identical to CVE-2023-3935	N/A	More Details
CVE-2023-41901	Rejected reason: Further research determined the issue is not a vulnerability.	N/A	More Details
CVE-2021-1842	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2023-1576	Rejected reason: This is a duplicate of an earlier CVE, CVE-2022-47069.	N/A	More Details
CVE-2008-7259	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2008-7260	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2009-3768	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2009-3769	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2009-3770	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2022-38636	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2009-3771	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2009-3772	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2023-3378	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2019-8899	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2009-3774	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2009-3775	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2009-3776	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2009-3777	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2010-0061	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2010-0499	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2010-1765	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2010-1779	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2010-1798	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2010-1826	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2023-4563	Rejected reason: This was assigned as a duplicate of CVE-2023-4244.	N/A	More Details
CVE-2010-1839	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8868	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8866	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4788	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4802	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4814	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4813	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4812	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4811	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4810	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4809	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4808	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4807	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4806	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4805	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4804	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4803	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4801	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4816	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4800	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4799	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4798	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4797	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4796	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4795	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4794	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4793	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4792	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4791	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4790	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4789	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4815	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4817	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8865	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-25079	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8864	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8863	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8862	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8861	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8860	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8859	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8845	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-8843	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-25083	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-25082	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-25081	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2019-25080	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4831	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4818	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4830	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4829	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4828	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4827	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4826	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4825	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4824	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4823	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4822	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4821	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4820	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4819	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4666	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4665	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4664	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5291	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5293	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5294	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5295	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5296	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5297	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5298	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5299	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2014-8841	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2014-8842	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2015-1160	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2015-20002	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2015-5762	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2015-7118	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2016-7704	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13893	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13894	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13895	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13896	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13897	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13898	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13899	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-13900	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13901	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5292	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5290	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5264	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5289	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5266	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5267	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5268	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5269	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5270	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5271	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5272	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2013-5273	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5274	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5275	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5276	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5277	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5278	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5279	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5280	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5281	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5282	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5283	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5284	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5285	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2013-5286	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5287	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5288	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13902	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13912	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13913	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13914	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13941	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13942	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13943	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13944	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13945	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13946	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-13947	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13948	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13949	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13950	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13951	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13952	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13953	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13954	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13955	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13956	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13957	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13958	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13959	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-13960	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13961	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13962	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13963	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13940	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13939	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13938	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13925	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13915	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13916	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13917	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13918	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13919	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-13920	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13921	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13922	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13923	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13924	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13926	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13937	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13927	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13928	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13929	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13930	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13931	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13932	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-13933	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13934	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13935	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13936	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5265	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5263	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4663	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2011-3470	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2011-3472	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2011-3473	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2011-3474	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2011-3475	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-0653	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2012-0673	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3619	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3662	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3717	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3759	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3760	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3761	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3762	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3763	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3764	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3765	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3766	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3767	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2012-3768	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3769	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3770	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3771	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3772	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2011-3471	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2011-3469	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5262	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2011-3468	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2010-3799	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2010-3807	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2010-3815	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2010-3825	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2010-4014	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2010-4016	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2010-4017	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2011-0171	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2011-0236	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2011-0239	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2011-0243	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2011-3240	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2011-3258	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2011-3433	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2011-3445	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2011-3451	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2011-3454	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2011-3455	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2011-3456	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2011-3461	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2011-3465	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2011-3466	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2011-3467	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3773	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3774	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3775	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3776	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5239	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5240	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5241	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2013-5242	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5243	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5244	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5245	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5246	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5247	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5248	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5249	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5250	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5251	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5252	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5253	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5254	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2013-5255	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5256	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5257	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5258	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5259	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5260	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5261	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5238	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5237	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5236	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3787	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3777	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3778	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2012-3779	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3780	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3781	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3782	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3783	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3784	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3785	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3786	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2012-3788	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5235	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-0965	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-0972	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5146	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2013-5194	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5226	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5230	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5231	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5232	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5233	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2013-5234	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13964	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13965	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13966	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4585	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4587	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4588	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4589	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4590	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4591	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4592	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4593	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4594	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4595	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4596	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4597	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4598	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4599	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4600	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4601	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4602	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4603	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4604	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4605	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4606	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4607	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4608	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4609	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4586	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4584	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13967	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4583	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4560	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4561	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4562	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4563	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4564	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4565	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4566	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4567	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4568	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4569	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4570	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4571	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4572	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4573	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4574	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4575	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4576	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4577	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4578	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4579	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4580	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4581	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4582	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4610	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4611	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4612	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4613	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4640	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4641	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4642	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4643	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4644	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4645	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4646	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4647	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4648	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4649	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4650	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4651	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4652	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4653	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4654	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4655	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4656	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4657	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4658	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4659	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4660	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4661	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4662	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4639	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4638	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4637	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4624	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4614	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2010-1827	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4616	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4617	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4618	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4619	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4620	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4621	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4622	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4623	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4625	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4636	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4626	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4627	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4628	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4629	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4630	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4631	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4632	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4633	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4634	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4635	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4559	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4558	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4557	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4504	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4480	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4481	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4482	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4483	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4484	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4485	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4486	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4487	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4488	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4489	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4490	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4491	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4492	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4493	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4494	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4495	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4496	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4497	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4498	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4499	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4500	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4501	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4502	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4479	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4477	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4476	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13978	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13968	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13969	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13970	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13971	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13972	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13973	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13974	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13975	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13976	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13977	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13979	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4475	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13980	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-13981	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-7166	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-7168	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2017-7169	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4466	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4469	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4471	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4472	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4473	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4503	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4505	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4556	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4506	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4533	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4534	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4535	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4536	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4537	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4538	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4539	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4540	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4541	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4542	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4543	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4544	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4545	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4546	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4547	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4548	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4549	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4550	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4551	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4552	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4553	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4554	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4555	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4532	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4531	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4530	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4517	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4507	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4508	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4509	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4510	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4511	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4512	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4513	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4514	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4515	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4516	Rejected reason: This candidate is unused by its CNA.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-4518	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4529	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4519	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4520	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4521	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4522	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4523	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4524	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4525	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4526	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4527	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4528	Rejected reason: This candidate is unused by its CNA.	N/A	More Details
CVE-2018-4615	Rejected reason: This candidate is unused by its CNA.	N/A	More Details