SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 01 March 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-2023-25813	Sequelize is a Node.js ORM tool. In versions prior to 6.19.1 a SQL injection exploit exists related to replacements. Parameters which are passed through replacements are not properly escaped which can lead to arbitrary SQL injection depending on the specific queries in use. The issue has been fixed in Sequelize 6.19.1. Users are advised to upgrade. Users unable to upgrade should not use the `replacements` and the `where` option in the same query.	10.0	More Details
CVE-2023-0947	Path Traversal in GitHub repository flatpressblog/flatpress prior to 1.3.	9.8	More Details
CVE-2023-25233	Tenda AC500 V2.0.1.9(1307) is vulnerable to Buffer Overflow in function fromRouteStatic via parameters entrys and mitInterface.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2024	OS Command Injection in GitHub repository gogs/gogs prior to 0.12.11.	9.8	More Details
CVE-2023-26550	A SQL injection vulnerability in BMC Control-M before 9.0.20.214 allows attackers to execute arbitrary SQL commands via the memname JSON field.	9.8	More Details
CVE-2023-26602	ASUS ASMB8 iKVM firmware through 1.14.51 allows remote attackers to execute arbitrary code by using SNMP to create extensions, as demonstrated by snmpset for NET-SNMP-EXTEND-MIB with /bin/sh for command execution.	9.8	More Details
CVE-2023-24206	Davinci v0.3.0-rc was discovered to contain a SQL injection vulnerability via the copyDisplay function.	9.8	More Details
CVE-2023-23080	Certain Tenda products are vulnerable to command injection. This affects Tenda CP7 Tenda CP7<=V11.10.00.2211041403 and Tenda CP3 v.10 Tenda CP3 v.10<=V20220906024_2025 and Tenda IT7-PCS Tenda IT7-PCS<=V2209020914 and Tenda IT7-LCS Tenda IT7-LCS<=V2209020914 and Tenda IT7-PRS Tenda IT7-PRS<=V2209020908.	9.8	More Details
CVE-2022-45138	The configuration backend of the web-based management can be used by unauthenticated users, although only authenticated users should be able to use the API. The vulnerability allows an unauthenticated attacker to read and set several device parameters that can lead to full compromise of the device.	9.8	More Details
CVE-2022-45140	The configuration backend allows an unauthenticated user to write arbitrary data with root privileges to the storage, which could lead to unauthenticated remote code execution and full system compromise.	9.8	More Details
CVE-2023-23155	Art Gallery Management System Project in PHP 1.0 was discovered to contain a SQL injection vulnerability via the username parameter in the Admin Login.	9.8	More Details
CVE-2023-23156	Art Gallery Management System Project in PHP 1.0 was discovered to contain a SQL injection vulnerability via the pid parameter in the single-product page.	9.8	More Details
CVE-2023-25231	Tenda Router W30E V1.0.1.25(633) is vulnerable to Buffer Overflow in function fromRouteStatic via parameters entrys and mitInterface.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25234	Tenda AC500 V2.0.1.9(1307) is vulnerable to Buffer Overflow in function fromAddressNat via parameters entrys and mitInterface.	9.8	More Details
CVE-2023-24107	hour_of_code_python_2015 commit 520929797b9ca43bb818b2e8f963fb2025459fa3 was discovered to contain a code execution backdoor via the request package (requirements.txt). This vulnerability allows attackers to access sensitive user information and execute arbitrary code.	9.8	More Details
CVE-2022-48255	There is a system command injection vulnerability in BiSheng-WNM FW 3.0.0.325. A Huawei printer has a system command injection vulnerability. Successful exploitation could lead to remote code execution.	9.8	More Details
CVE-2022-48259	There is a system command injection vulnerability in BiSheng-WNM FW 3.0.0.325. Successful exploitation could allow attackers to gain higher privileges.	9.8	More Details
CVE-2022-48283	A piece of Huawei whole-home intelligence software has an Incorrect Privilege Assignment vulnerability. Successful exploitation of this vulnerability could allow attackers to access restricted functions.	9.8	More Details
CVE-2022-48284	A piece of Huawei whole-home intelligence software has an Incorrect Privilege Assignment vulnerability. Successful exploitation of this vulnerability could allow attackers to access restricted functions.	9.8	More Details
CVE-2023-24253	Domotica Labs srl Ikon Server before v2.8.6 was discovered to contain a SQL injection vulnerability.	9.8	More Details
CVE-2022-26760	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 15.5 and iPadOS 15.5. A malicious application may be able to elevate privileges.	9.8	More Details
CVE-2022-46723	This issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.6.1, macOS Big Sur 11.7.1. A remote user may be able to write arbitrary files.	9.8	More Details
CVE-2023-23513	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Big Sur 11.7.3, macOS Ventura 13.2, macOS Monterey 12.6.3. Mounting a maliciously crafted Samba network share may lead to arbitrary code execution.	9.8	More Details
CVE-2023-24258	SPIP v4.1.5 and earlier was discovered to contain a SQL injection vulnerability via the _oups parameter. This vulnerability allows attackers to execute arbitrary code via a crafted POST request.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20946	In onStart of BluetoothSwitchPreferenceController.java, there is a possible permission bypass due to a confused deputy. This could lead to remote escalation of privilege in Bluetooth settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-244423101	9.8	More Details
CVE-2023-24189	An XML External Entity (XXE) vulnerability in urule v2.1.7 allows attackers to execute arbitrary code via uploading a crafted XML file to /urule/common/saveFile.	9.8	More Details
CVE-2021-35370	An issue found in Peacexie Imcat v5.4 allows attackers to execute arbitrary code via the incomplete filtering function.	9.8	More Details
CVE-2023-27372	SPIP before 4.2.1 allows Remote Code Execution via form values in the public area because serialization is mishandled. The fixed versions are 3.2.18, 4.0.10, 4.1.8, and 4.2.1.	9.8	More Details
CVE-2023-24114	typecho 1.1/17.10.30 was discovered to contain a remote code execution (RCE) vulnerability via install.php.	9.8	More Details
CVE-2022-45599	Aztech WMB250AC Mesh Routers Firmware Version 016 2020 is vulnerable to PHP Type Juggling in file /var/www/login.php, allows attackers to gain escalated privileges only when specific conditions regarding a given accounts hashed password.	9.8	More Details
CVE-2022-48149	Online Student Admission System in PHP Free Source Code 1.0 was discovered to contain a SQL injection vulnerability via the username parameter.	9.8	More Details
CVE-2023-0939	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in NTN Information Technologies Online Services Software allows SQL Injection.This issue affects Online Services Software: before 1.17.	9.8	More Details
CVE-2022-2504	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in SDD Computer Software SDD-Baro allows SQL Injection.This issue affects SDD-Baro: before 2.8.432.	9.8	More Details
CVE-2023-24104	Ubiquiti Networks UniFi Dream Machine Pro v7.2.95 allows attackers to bypass domain restrictions via crafted packets.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33224	File upload vulnerability in Umbraco Forms v.8.7.0 allows unauthenticated attackers to execute arbitrary code via a crafted web.config and asp file.	9.8	More Details
CVE-2023-26326	The BuddyForms WordPress plugin, in versions prior to 2.7.8, was affected by an unauthenticated insecure deserialization issue. An unauthenticated attacker could leverage this issue to call files using a PHAR wrapper that will deserialize the data and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present.	9.8	More Details
CVE-2022-36231	pdf_info 0.5.3 is vulnerable to Command Execution because the Ruby code uses backticks instead of Open3.	9.8	More Details
CVE-2023-0754	The affected products are vulnerable to an integer overflow or wraparound, which could allow an attacker to crash the server and remotely execute arbitrary code.	9.8	More Details
CVE-2023-0755	The affected products are vulnerable to an improper validation of array index, which could allow an attacker to crash the server and remotely execute arbitrary code.	9.8	More Details
CVE-2023-24205	Clash for Windows v0.20.12 was discovered to contain a remote code execution (RCE) vulnerability which is exploited via overwriting the configuration file (cfw-setting.yaml).	9.8	More Details
CVE-2023-24212	Tenda AX3 V16.03.12.11 was discovered to contain a stack overflow via the timeType function at /goform/SetSysTimeCfg.	9.8	More Details
CVE-2023-24093	An access control issue in H3C A210-G A210-GV100R005 allows attackers to authenticate without a password.	9.8	More Details
CVE-2021-4105	Improper Handling of Parameters vulnerability in BG-TEK COSLAT Firewall allows Remote Code Inclusion.This issue affects COSLAT Firewall: from 5.24.0.R.20180630 before 5.24.0.R.20210727.	9.8	More Details
CVE-2022-41217	Cloudflow contains a unauthenticated file upload vulnerability, which makes it possible for an attacker to upload malicious files to the CLOUDFLOW PROOFSCOPE built-in storage.	9.8	More Details
CVE-2023-25691	Improper Input Validation vulnerability in the Apache Airflow Google Provider. This issue affects Apache Airflow Google Provider versions before 8.10.0.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25693	Improper Input Validation vulnerability in the Apache Airflow Sqoop Provider. This issue affects Apache Airflow Sqoop Provider versions before 3.1.1.	9.8	More Details
CVE-2023-24108	MvcTools 6d48cd6830fc1df1d8c9d61caa1805fd6a1b7737 was discovered to contain a code execution backdoor via the request package (requirements.txt). This vulnerability allows attackers to access sensitive user information and execute arbitrary code.	9.8	More Details
CVE-2023-25696	Improper Input Validation vulnerability in the Apache Airflow Hive Provider. This issue affects Apache Airflow Hive Provider versions before 5.1.3.	9.8	More Details
CVE-2022-39983	File upload vulnerability in Instantdeveloper RD3 22.0.8500, allows attackers to execute arbitrary code.	9.8	More Details
CVE-2021-33387	Cross Site Scripting Vulnerability in MiniCMS v.1.10 allows attacker to execute arbitrary code via a crafted get request.	9.6	More Details
CVE-2021-3329	Lack of proper validation in HCI Host stack initialization can cause a crash of the bluetooth stack	9.6	More Details
CVE-2023-26034	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 are affected by a SQL Injection vulnerability. The (blind) SQL Injection vulnerability is present within the `filter[Query][terms][0][attr]` query string parameter of the `/zm/index.php` endpoint. A user with the View or Edit permissions of Events may execute arbitrary SQL. The resulting impact can include unauthorized data access (and modification), authentication and/or authorization bypass, and remote code execution.	9.6	More Details
CVE-2023-0104	The listed versions for Weintek EasyBuilder Pro are vulnerable to a ZipSlip attack caused by decompiling a malicious project file. This may allow an attacker to gain control of the user's computer or gain access to sensitive data.	9.3	More Details
CVE-2023-26468	Cerebrate 1.12 does not properly consider organisation_id during creation of API keys.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0339	Relative Path Traversal vulnerability in ForgeRock Access Management Web Policy Agent allows Authentication Bypass. This issue affects Access Management Web Policy Agent: all versions up to 5.10.1	9.1	More Details
CVE-2023-0511	Relative Path Traversal vulnerability in ForgeRock Access Management Java Policy Agent allows Authentication Bypass. This issue affects Access Management Java Policy Agent: all versions up to 5.10.1	9.1	More Details
CVE-2023-23914	A cleartext transmission of sensitive information vulnerability exists in curl <v7.88.0 that could cause HSTS functionality fail when multiple URLs are requested serially. Using its HSTS support, curl can be instructed to use HTTPS instead of usingan insecure clear-text HTTP step even when HTTP is provided in the URL. ThisHSTS mechanism would however surprisingly be ignored by subsequent transferswhen done on the same command line because the state would not be properlycarried on.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-26032	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain SQL Injection via malicious jason web token. The Username field of the JWT token was trusted when performing an SQL query to load the user. If an attacker could determine the HASH key used by ZoneMinder, they could generate a malicious JWT token and use it to execute arbitrary SQL. This issue is fixed in versions 1.36.33 and 1.37.33.	8.9	More Details
CVE-2023-26037	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain an SQL Injection. The minTime and maxTime request parameters are not properly validated and could be used execute arbitrary SQL. This issue is fixed in versions 1.36.33 and 1.37.33.	8.9	More Details
CVE-2023-23917	A prototype pollution vulnerability exists in Rocket.Chat server <5.2.0 that could allow an attacker to a RCE under the admin account. Any user can create their own server in your cloud and become an admin so this vulnerability could affect the cloud infrastructure. This attack vector also may increase the impact of XSS to RCE which is dangerous for self-hosted users as well.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42826	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13, iOS 16.1 and iPadOS 16, Safari 16.1. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2023-0928	Use after free in SwiftShader in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-0929	Use after free in Vulkan in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-0931	Use after free in Video in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-0932	Use after free in WebRTC in Google Chrome on Windows prior to 110.0.5481.177 allowed a remote attacker who convinced the user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-0933	Integer overflow in PDF in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-0941	Use after free in Prompts in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2023-1034	Path Traversal: '\..\filename' in GitHub repository salesagility/suitecrm prior to 7.12.9.	8.8	More Details
CVE-2023-24812	Misskey is an open source, decentralized social media platform. In versions prior to 13.3.3 SQL injection is possible due to insufficient parameter validation in the note search API by tag (notes/search-by-tag). This has been fixed in version 13.3.3. Users are advised to upgrade. Users unable to upgrade should block access to the `api/notes/search-by-tag` endpoint.	8.8	More Details
CVE-2023-1033	Cross-Site Request Forgery (CSRF) in GitHub repository froxlor/froxlor prior to 2.0.11.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22973	A Local File Inclusion (LFI) vulnerability in interface/forms/LBF/new.php in OpenEMR < 7.0.0 allows remote authenticated users to execute code via the formname parameter.	8.8	More Details
CVE-2021-34167	Cross Site Request Forgery (CSRF) vulnerability in taoCMS 3.0.2 allows remote attackers to gain escalated privileges via taocms/admin/admin.php.	8.8	More Details
CVE-2022-45600	Aztech WMB250AC Mesh Routers Firmware Version 016 2020 devices improperly manage sessions, which allows remote attackers to bypass authentication in opportunistic circumstances and execute arbitrary commands with administrator privileges by leveraging an existing web portal login.	8.8	More Details
CVE-2023-23295	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root.	8.8	More Details
CVE-2023-23294	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root.	8.8	More Details
CVE-2023-26325	The 'rx_export_review' action in the ReviewX WordPress Plugin, is affected by an authenticated SQL injection vulnerability in the 'filterValue' and 'selectedColumns' parameters.	8.8	More Details
CVE-2023-20011	A vulnerability in the web-based management interface of Cisco Application Policy Infrastructure Controller (APIC) and Cisco Cloud Network Controller, formerly Cisco Cloud APIC, could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface on an affected system. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user. If the affected user has administrative privileges, these actions could include modifying the system configuration and creating new privileged accounts.	8.8	More Details
CVE-2023-23496	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.2, watchOS 9.3, iOS 15.7.2 and iPadOS 15.7.2, Safari 16.3, tvOS 16.3, iOS 16.3 and iPadOS 16.3. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48341	ThingsBoard 3.4.1 could allow a remote authenticated attacker to achieve Vertical Privilege Escalation. A Tenant Administrator can obtain System Administrator dashboard access by modifying the scope via the scopes parameter.	8.8	More Details
CVE-2023-23529	A type confusion issue was addressed with improved checks. This issue is fixed in iOS 15.7.4 and iPadOS 15.7.4, iOS 16.3.1 and iPadOS 16.3.1, macOS Ventura 13.2.1, Safari 16.3. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.	8.8	More Details
CVE-2023-23518	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.6.3, macOS Ventura 13.2, watchOS 9.3, macOS Big Sur 11.7.3, Safari 16.3, tvOS 16.3, iOS 16.3 and iPadOS 16.3. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2023-0927	Use after free in Web Payments API in Google Chrome on Android prior to 110.0.5481.177 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-0930	Heap buffer overflow in Video in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-25266	An issue was discovered in Docmosis Tornado prior to version 2.9.5. An authenticated attacker can change the Office directory setting pointing to an arbitrary remote network path. This triggers the execution of the soffice binary under the attackers control leading to arbitrary remote code execution (RCE).	8.8	More Details
CVE-2023-0381	The GigPress WordPress plugin through 2.3.28 does not validate and escape some of its shortcode attributes before using them in SQL statement/s, which could allow any authenticated users, such as subscriber to perform SQL Injection attacks	8.8	More Details
CVE-2023-20855	VMware vRealize Orchestrator contains an XML External Entity (XXE) vulnerability. A malicious actor, with non-administrative access to vRealize Orchestrator, may be able to use specially crafted input to bypass XML parsing restrictions leading to access to sensitive information or possible escalation of privileges.	8.8	More Details
CVE-2023-26762	Sme.UP ERP TOKYO V6R1M220406 was discovered to contain an arbitrary file upload vulnerability.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26759	Sme.UP ERP TOKYO V6R1M220406 was discovered to contain an OS command injection vulnerability via calls made to the XMService component.	8.8	More Details
CVE-2023-26314	The mono package before 6.8.0.105+dfsg-3.3 for Debian allows arbitrary code execution because the application/x-ms-dos-executable MIME type is associated with an un-sandboxed Mono CLR interpreter.	8.8	More Details
CVE-2023-24656	Simple Customer Relationship Management System v1.0 was discovered to contain a SQL injection vulnerability via the subject parameter under the Create Ticket function.	8.8	More Details
CVE-2023-24654	Simple Customer Relationship Management System v1.0 was discovered to contain a SQL injection vulnerability via the name parameter under the Request a Quote function.	8.8	More Details
CVE-2023-24653	Simple Customer Relationship Management System v1.0 was discovered to contain a SQL injection vulnerability via the oldpass parameter under the Change Password function.	8.8	More Details
CVE-2023-24652	Simple Customer Relationship Management System v1.0 was discovered to contain a SQL injection vulnerability via the Description parameter under the Create ticket function.	8.8	More Details
CVE-2022-48362	Zoho ManageEngine Desktop Central and Desktop Central MSP before 10.1.2137.2 allow directory traversal via computerName to AgentLogUploadServlet. A remote, authenticated attacker could upload arbitrary code that would be executed when Desktop Central is restarted. (The attacker could authenticate by exploiting CVE-2021-44515.)	8.8	More Details
CVE-2023-24364	Simple Customer Relationship Management System v1.0 was discovered to contain a SQL injection vulnerability via the username parameter under the Admin Panel.	8.8	More Details
CVE-2023-23517	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.6.3, macOS Ventura 13.2, watchOS 9.3, macOS Big Sur 11.7.3, Safari 16.3, tvOS 16.3, iOS 16.3 and iPadOS 16.3. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41565	The Web Application component of TIBCO Software Inc.'s TIBCO EBX and TIBCO Product and Service Catalog powered by TIBCO EBX contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute a stored XSS on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO EBX: versions 5.9.21 and below, versions 6.0.11 and below and TIBCO Product and Service Catalog powered by TIBCO EBX: versions 1.2.0 and below.	8.7	More Details
CVE-2022-41566	The server component of TIBCO Software Inc.'s TIBCO EBX Add-ons contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute stored XSS on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO EBX Add-ons: versions 5.6.0 and below.	8.7	More Details
CVE-2022-4895	Improper Certificate Validation vulnerability in Hitachi Infrastructure Analytics Advisor on Linux (Analytics probe component), Hitachi Ops Center Analyzer on Linux (Analyzer probe component) allows Man in the Middle Attack.This issue affects Hitachi Infrastructure Analytics Advisor: from 2.0.0-00 through 4.4.0-00; Hitachi Ops Center Analyzer: from 10.0.0-00 before 10.9.1-00.	8.6	More Details
CVE-2023-23530	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges.	8.6	More Details
CVE-2023-23531	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges.	8.6	More Details
CVE-2022-41216	Local File Inclusion vulnerability within Cloudflow allows attackers to retrieve confidential information from the system.	8.3	More Details
CVE-2022-34908	An issue was discovered in the A4N (Aremis 4 Nomad) application 1.5.0 for Android. It possesses an authentication mechanism; however, some features do not require any token or cookie in a request. Therefore, an attacker may send a simple HTTP request to the right endpoint, and obtain authorization to retrieve application data.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26036	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain a Local File Inclusion (Untrusted Search Path) vulnerability via /web/index.php. By controlling $view, any local file ending in .php can be executed. This is supposed to be mitigated by calling detaintPath, however dentaintPath does not properly sandbox the path. This can be exploited by constructing paths like "..././", which get replaced by "../". This issue is patched in versions 1.36.33 and 1.37.33.	8.1	More Details
CVE-2023-24317	Judging Management System 1.0 was discovered to contain an arbitrary file upload vulnerability via the component edit_organizer.php.	8.1	More Details
CVE-2023-26462	ThingsBoard 3.4.1 could allow a remote attacker to gain elevated privileges because hard-coded service credentials (usable for privilege escalation) are stored in an insecure format. (To read this stored data, the attacker needs access to the application server or its source code.)	8.1	More Details
CVE-2023-22995	In the Linux kernel before 5.17, an error path in dwc3_qcom_acpi_register_core in drivers/usb/dwc3/dwc3-qcom.c lacks certain platform_device_put and kfree calls.	7.8	More Details
CVE-2023-20945	In phNciNfc_MfCreateXchgDataHdr of phNxpExtns_MifareStd.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-246932269	7.8	More Details
CVE-2023-20943	In clearApplicationUserData of ActivityManagerService.java, there is a possible way to remove system files due to a path traversal error. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-240267890	7.8	More Details
CVE-2023-20938	In binder_transaction_buffer_release of binder.c, there is a possible use after free due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-257685302References: Upstream kernel	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20937	In several functions of the Android Linux kernel, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-257443051References: Upstream kernel	7.8	More Details
CVE-2023-20944	In run of ChooseTypeAndAccountActivity.java, there is a possible escalation of privilege due to unsafe deserialization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-244154558	7.8	More Details
CVE-2023-20934	In resolveAttributionSource of ServiceUtilities.cpp, there is a possible way to disable the microphone privacy indicator due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-258672042	7.8	More Details
CVE-2023-23514	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 16.3.1 and iPadOS 16.3.1, macOS Ventura 13.2.1, macOS Big Sur 11.7.5. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-20933	In several functions of MediaCodec.cpp, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-245860753	7.8	More Details
CVE-2023-0461	There is a use-after-free vulnerability in the Linux Kernel which can be exploited to achieve local privilege escalation. To reach the vulnerability kernel configuration flag CONFIG_TLS or CONFIG_XFRM_ESPINTCP has to be configured, but the operation does not require any privilege. There is a use-after-free bug of icsk_ulp_data of a struct inet_connection_sock. When CONFIG_TLS is enabled, user can install a tls context (struct tls_context) on a connected tcp socket. The context is not cleared if this socket is disconnected and reused as a listener. If a new socket is created from the listener, the context is inherited and vulnerable. The setsockopt TCP_ULP operation does not require any privilege. We recommend upgrading past commit 2c02d41d71f90a5168391b6a5f2954112ba2307c	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20940	In the Android operating system, there is a possible way to replace a boot partition due to improperly used crypto. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-256237041	7.8	More Details
CVE-2023-23507	The issue was addressed with improved bounds checks. This issue is fixed in macOS Monterey 12.6.3, macOS Ventura 13.2. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-23504	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.6.3, macOS Ventura 13.2, watchOS 9.3, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-32900	A logic issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.6, macOS Big Sur 11.7. An app may be able to gain elevated privileges.	7.8	More Details
CVE-2022-45697	Arbitrary File Delete vulnerability in Razer Central before v7.8.0.381 when handling files in the Accounts directory.	7.8	More Details
CVE-2023-26606	In the Linux kernel 6.0.8, there is a use-after-free in ntfs_trim_fs in fs/ntfs3/bitmap.c.	7.8	More Details
CVE-2023-26605	In the Linux kernel 6.0.8, there is a use-after-free in inode_cgwb_move_to_attached in fs/fs-writeback.c, related to __list_del_entry_valid.	7.8	More Details
CVE-2022-32949	This issue was addressed with improved checks. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, tvOS 16. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-42797	An injection issue was addressed with improved input validation. This issue is fixed in Xcode 14.1. An app may be able to gain root privileges.	7.8	More Details
CVE-2023-26544	In the Linux kernel 6.0.8, there is a use-after-free in run_unpack in fs/ntfs3/run.c, related to a difference between NTFS sector size and media sector size.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20939	In multiple functions of looper_backed_event_loop.cpp, there is a possible way to corrupt memory due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-243362981	7.8	More Details
CVE-2022-42833	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-46712	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13. An app may be able to cause unexpected system termination or potentially execute code with kernel privileges.	7.8	More Details
CVE-2023-0996	There is a vulnerability in the strided image data parsing code in the emscripten wrapper for libheif. An attacker could exploit this through a crafted image file to cause a buffer overflow in linear memory during a memcpy call.	7.8	More Details
CVE-2023-23497	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.7.3, macOS Ventura 13.2, macOS Monterey 12.6.3. An app may be able to gain root privileges.	7.8	More Details
CVE-2023-1017	An out-of-bounds write vulnerability exists in TPM2.0's Module Library allowing writing of a 2-byte data past the end of TPM2.0 command in the CryptParameterDecryption routine. An attacker who can successfully exploit this vulnerability can lead to denial of service (crashing the TPM chip/process or rendering it unusable) and/or arbitrary code execution in the TPM context.	7.8	More Details
CVE-2022-34909	An issue was discovered in the A4N (Aremis 4 Nomad) application 1.5.0 for Android. It allows SQL Injection, by which an attacker can bypass authentication and retrieve data that is stored in the database.	7.7	More Details
CVE-2023-25825	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 are vulnerable to Cross-site Scripting. Log entries can be injected into the database logs, containing a malicious referrer field. This is unescaped when viewing the logs in the web ui. This issue is patched in version 1.36.33.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25575	API Platform Core is the server component of API Platform: hypermedia and GraphQL APIs. Resource properties secured with the `security` option of the `ApiPlatform\Metadata\ApiProperty` attribute can be disclosed to unauthorized users. The problem affects most serialization formats, including raw JSON, which is enabled by default when installing API Platform. Custom serialization formats may also be impacted. Only collection endpoints are affected by the issue, item endpoints are not. The JSON-LD format is not affected by the issue. The result of the security rule is only executed for the first item of the collection. The result of the rule is then cached and reused for the next items. This bug can leak data to unauthorized users when the rule depends on the value of a property of the item. This bug can also hide properties that should be displayed to authorized users. This issue impacts the 2.7, 3.0 and 3.1 branches. Please upgrade to versions 2.7.10, 3.0.12 or 3.1.3. As a workaround, replace the `cache_key` of the context array of the Serializer inside a custom normalizer that works on objects if the security option of the `ApiPlatform\Metadata\ApiProperty` attribute is used.	7.7	More Details
CVE-2023-20948	In dropFramesUntilIframe of AAVCAssembler.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-230630526	7.5	More Details
CVE-2023-26105	All versions of the package utilities are vulnerable to Prototype Pollution via the _mix function.	7.5	More Details
CVE-2022-41722	A path traversal vulnerability exists in filepath.Clean on Windows. On Windows, the filepath.Clean function could transform an invalid path such as "a/../c:/b" into the valid path "c:\b". This transformation of a relative (if invalid) path into an absolute path could enable a directory traversal attack. After fix, the filepath.Clean function transforms this path into the relative (but still invalid) path ".\c:\b".	7.5	More Details
CVE-2022-41723	A maliciously crafted HTTP/2 stream could cause excessive CPU consumption in the HPACK decoder, sufficient to cause a denial of service from a small number of small requests.	7.5	More Details
CVE-2022-41724	Large handshake records may cause panics in crypto/tls. Both clients and servers may send large TLS handshake records which cause servers and clients, respectively, to panic when attempting to construct responses. This affects all TLS 1.3 clients, TLS 1.2 clients which explicitly enable session resumption (by setting Config.ClientSessionCache to a non-nil value), and TLS 1.3 servers which request client certificates (by setting Config.ClientAuth >= RequestClientCert).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41725	A denial of service is possible from excessive resource consumption in net/http and mime/multipart. Multipart form parsing with mime/multipart.Reader.ReadForm can consume largely unlimited amounts of memory and disk files. This also affects form parsing in the net/http package with the Request methods FormFile, FormValue, ParseMultipartForm, and PostFormValue. ReadForm takes a maxMemory parameter, and is documented as storing "up to maxMemory bytes +10MB (reserved for non-file parts) in memory". File parts which cannot be stored in memory are stored on disk in temporary files. The unconfigurable 10MB reserved for non-file parts is excessively large and can potentially open a denial of service vector on its own. However, ReadForm did not properly account for all memory consumed by a parsed form, such as map entry overhead, part names, and MIME headers, permitting a maliciously crafted form to consume well over 10MB. In addition, ReadForm contained no limit on the number of disk files created, permitting a relatively small request body to create a large number of disk temporary files. With fix, ReadForm now properly accounts for various forms of memory overhead, and should now stay within its documented limit of 10MB + maxMemory bytes of memory consumption. Users should still be aware that this limit is high and may still be hazardous. In addition, ReadForm now creates at most one on-disk temporary file, combining multiple form parts into a single temporary file. The mime/multipart.File interface type's documentation states, "If stored on disk, the File's underlying concrete type will be an *os.File.". This is no longer the case when a form contains more than one file part, due to this coalescing of parts into a single file. The previous behavior of using distinct files for each form part may be reenabled with the environment variable GODEBUG=multipartfiles=distinct. Users should be aware that multipart.ReadForm and the http.Request methods that call it do not limit the amount of disk consumed by temporary files. Callers can limit the size of form data with http.MaxBytesReader.	7.5	More Details
CVE-2023-23524	A denial-of-service issue was addressed with improved input validation. This issue is fixed in tvOS 16.3.2, iOS 16.3.1 and iPadOS 16.3.1, watchOS 9.3.1, macOS Ventura 13.2.1. Processing a maliciously crafted certificate may lead to a denial-of-service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23109	In crasm 1.8-3, invalid input validation, specific files passed to the command line application, can lead to a divide by zero fault in the function opdiv.	7.5	More Details
CVE-2023-23519	A memory corruption issue was addressed with improved state management. This issue is fixed in watchOS 9.3, tvOS 16.3, macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. Processing an image may lead to a denial-of-service.	7.5	More Details
CVE-2023-23108	In crasm 1.8-3, invalid input validation, specific files passed to the command line application, can lead to a NULL pointer dereference in the function Xasc.	7.5	More Details
CVE-2023-25824	Mod_gnutls is a TLS module for Apache HTTPD based on GnuTLS. Versions from 0.9.0 to 0.12.0 (including) did not properly fail blocking read operations on TLS connections when the transport hit timeouts. Instead it entered an endless loop retrying the read operation, consuming CPU resources. This could be exploited for denial of service attacks. If trace level logging was enabled, it would also produce an excessive amount of log output during the loop, consuming disk space. The problem has been fixed in commit d7eec4e598158ab6a98bf505354e84352f9715ec, please update to version 0.12.1. There are no workarounds, users who cannot update should apply the errno fix detailed in the security advisory.	7.5	More Details
CVE-2023-26257	An issue was discovered in the Connected Vehicle Systems Alliance (COVESA; formerly GENIVI) dlt-daemon through 2.18.8. Dynamic memory is not released after it is allocated in dlt-control-common.c.	7.5	More Details
CVE-2022-48363	In MPD before 0.23.8, as used on Automotive Grade Linux and other platforms, the PipeWire output plugin mishandles a Drain call in certain situations involving truncated files. Eventually there is an assertion failure in libmpdclient because libqtappfw passes in a NULL pointer.	7.5	More Details
CVE-2023-26104	All versions of the package lite-web-server are vulnerable to Denial of Service (DoS) when an attacker sends an HTTP request and includes control characters that the decodeURI() function is unable to parse.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26033	Gentoo soko is the code that powers packages.gentoo.org. Versions prior to 1.0.1 are vulnerable to SQL Injection, leading to a Denial of Service. If the user selects (in user preferences) the "Recently Visited Packages" view for the index page, the value of the `search_history` cookie is used as a base64 encoded comma separated list of atoms. These are string loaded directly into the SQL query with `atom = '%s'` format string. As a result, any user can modify the browser's cookie value and inject most SQL queries. A proof of concept malformed cookie was generated that wiped the database or changed it's content. On the database, only public data is stored, so there is no confidentiality issues to site users. If it is known that the database was modified, a full restoration of data is possible by performing a full database wipe and performing full update of all components. This issue is patched with commit id 5ae9ca83b73. Version 1.0.1 contains the patch. If users are unable to upgrade immediately, the following workarounds may be applied: (1.) Use a proxy to always drop the `search_history` cookie until upgraded. The impact on user experience is low. (2.) Sanitize to the value of `search_history` cookie after base64 decoding it.	7.5	More Details
CVE-2021-34249	SQL injection vulnerability in sourcecodester online-book-store 1.0 allows remote attackers to view sensitive information via the id paremeter in application URL.	7.5	More Details
CVE-2023-22974	A Path Traversal in setup.php in OpenEMR < 7.0.0 allows remote unauthenticated users to read arbitrary files by controlling a connection to an attacker-controlled MySQL server.	7.5	More Details
CVE-2022-47076	An issue was discovered in Smart Office Web 20.28 and earlier allows attackers to view sensitive information via DisplayParallelLogData.aspx.	7.5	More Details
CVE-2022-44310	In Development IL ecdh before 0.2.0, an attacker can send an invalid point (not on the curve) as the public key, and obtain the derived shared secret.	7.5	More Details
CVE-2023-25956	Generation of Error Message Containing Sensitive Information vulnerability in the Apache Airflow AWS Provider. This issue affects Apache Airflow AWS Provider versions before 7.2.1.	7.5	More Details
CVE-2023-25692	Improper Input Validation vulnerability in the Apache Airflow Google Provider. This issue affects Apache Airflow Google Provider versions before 8.10.0.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4492	The undertow client is not checking the server identity presented by the server certificate in https connections. This is a compulsory step (at least it should be performed by default) in https and in http/2. I would add it to any TLS client protocol.	7.5	More Details
CVE-2022-47075	An issue was discovered in Smart Office Web 20.28 and earlier allows attackers to download sensitive information via the action name parameter to ExportEmployeeDetails.aspx, and to ExportReportingManager.aspx.	7.5	More Details
CVE-2023-26102	All versions of the package rangy are vulnerable to Prototype Pollution when using the extend() function in file rangy-core.js.The function uses recursive merge which can lead an attacker to modify properties of the Object.prototype	7.5	More Details
CVE-2023-0994	Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository francoisjacquet/rosariosis prior to 10.8.2.	7.5	More Details
CVE-2022-48230	There is a misinterpretation of input vulnerability in BiSheng-WNM FW 3.0.0.325. Successful exploitation could lead to DoS.	7.5	More Details
CVE-2023-23918	A privilege escalation vulnerability exists in Node.js <19.6.1, <18.14.1, <16.19.1 and <14.21.3 that made it possible to bypass the experimental Permissions (https://nodejs.org/api/permissions.html) feature in Node.js and access non authorized modules by using process.mainModule.require(). This only affects users who had enabled the experimental permissions option with --experimental-policy.	7.5	More Details
CVE-2022-4550	The User Activity WordPress plugin through 1.0.1 checks headers such as the X-Forwarded-For to retrieve the IP address of the request, which could lead to IP spoofing	7.5	More Details
CVE-2023-23919	A cryptographic vulnerability exists in Node.js <19.2.0, <18.14.1, <16.19.1, <14.21.3 that in some cases did does not clear the OpenSSL error stack after operations that may set it. This may lead to false positive errors during subsequent cryptographic operations that happen to be on the same thread. This in turn could be used to cause a denial of service.	7.5	More Details
CVE-2023-26758	Sme.UP TOKYO V6R1M220406 was discovered to contain an arbitrary file download vulnerabilty via the component /ResourceService.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25265	Docmosis Tornado <= 2.9.4 is vulnerable to Directory Traversal leading to the disclosure of arbitrary content on the file system.	7.5	More Details
CVE-2023-0331	The Correos Oficial WordPress plugin through 1.2.0.2 does not have an authorization check user input validation when generating a file path, allowing unauthenticated attackers to download arbitrary files from the server.	7.5	More Details
CVE-2022-32846	A logic issue was addressed with improved state management. This issue is fixed in Apple Music 3.9.10 for Android. An app may be able to access user-sensitive data.	7.5	More Details
CVE-2022-32836	This issue was addressed with improved state management. This issue is fixed in Apple Music 3.9.10 for Android. An app may be able to access user-sensitive data.	7.5	More Details
CVE-2023-26256	An unauthenticated path traversal vulnerability affects the "STAGIL Navigation for Jira - Menu & Themes" plugin before 2.0.52 for Jira. By modifying the fileName parameter to the snjFooterNavigationConfig endpoint, it is possible to traverse and read the file system.	7.5	More Details
CVE-2022-48260	There is a buffer overflow vulnerability in BiSheng-WNM FW 3.0.0.325. Successful exploitation could lead to device service exceptions.	7.5	More Details
CVE-2023-26760	Sme.UP ERP TOKYO V6R1M220406 was discovered to contain an information disclosure vulnerability via the /debug endpoint. This vulnerability allows attackers to access cleartext credentials needed to authenticate to the AS400 system.	7.5	More Details
CVE-2023-26255	An unauthenticated path traversal vulnerability affects the "STAGIL Navigation for Jira - Menu & Themes" plugin before 2.0.52 for Jira. By modifying the fileName parameter to the snjCustomDesignConfig endpoint, it is possible to traverse and read the file system.	7.5	More Details
CVE-2022-48261	There is a misinterpretation of input vulnerability in BiSheng-WNM FW 3.0.0.325. Successful exploitation of this vulnerability may cause the printer service to be abnormal.	7.5	More Details
CVE-2023-25264	An issue was discovered in Docmosis Tornado prior to version 2.9.5. An unauthenticated attacker can bypass the authentication check filter completely by introducing a specially crafted request with relative path segments.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2883	In affected versions of Octopus Deploy it is possible to upload a zipbomb file as a task which results in Denial of Service	7.5	More Details
CVE-2023-23040	TP-Link router TL-WR940N V6 3.19.1 Build 180119 uses a deprecated MD5 algorithm to hash the admin password used for basic authentication.	7.5	More Details
CVE-2023-23063	Cellinx NVT v1.0.6.002b was discovered to contain a local file disclosure vulnerability via the component /cgi-bin/GetFileContent.cgi.	7.5	More Details
CVE-2022-32830	An out-of-bounds read issue was addressed with improved bounds checking. This issue is fixed in tvOS 15.6, iOS 15.6 and iPadOS 15.6. Processing a maliciously crafted image may lead to disclosure of user information.	7.5	More Details
CVE-2023-25235	Tenda AC500 V2.0.1.9(1307) is vulnerable to Buffer Overflow in function formOneSsidCfgSet via parameter ssid.	7.5	More Details
CVE-2023-20089	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required.	7.4	More Details
CVE-2023-0963	A vulnerability was found in SourceCodester Music Gallery Site 1.0. It has been rated as critical. This issue affects some unknown processing of the file Users.php of the component POST Request Handler. The manipulation leads to improper access controls. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-221633 was assigned to this vulnerability.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26214	The BusinessConnect UI component of TIBCO Software Inc.'s TIBCO BusinessConnect contains easily exploitable Reflected Cross Site Scripting (XSS) vulnerabilities that allow a low privileged attacker with network access to execute scripts targeting the affected system or the victim's local system. Affected releases are TIBCO Software Inc.'s TIBCO BusinessConnect: versions 7.3.0 and below.	7.3	More Details
CVE-2023-1058	A vulnerability classified as critical has been found in SourceCodester Doctors Appointment System 1.0. This affects an unknown part of the file create-account.php. The manipulation of the argument newemail 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 associated identifier of this vulnerability is VDB-221823.	7.3	More Details
CVE-2022-41567	The BusinessConnect UI component of TIBCO Software Inc.'s TIBCO BusinessConnect contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute a cross-site scripting (XSS) attack on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO BusinessConnect: versions 7.3.0 and below.	7.3	More Details
CVE-2015-10086	A vulnerability, which was classified as critical, was found in OpenCycleCompass server-php. Affected is an unknown function of the file api1/login.php. The manipulation of the argument user leads to sql injection. It is possible to launch the attack remotely. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The name of the patch is fa0d9bcf81c711a88172ad0d37a842f029ac3782. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-221808.	7.3	More Details
CVE-2022-23535	LiteDB is a small, fast and lightweight .NET NoSQL embedded database. Versions prior to 5.0.13 are subject to Deserialization of Untrusted Data. LiteDB uses a special field in JSON documents to cast different types from `BsonDocument` to POCO classes. When instances of an object are not the same of class, `BsonMapper` use a special field `_type` string info with full class name with assembly to be loaded and fit into your model. If your end-user can send to your app a plain JSON string, deserialization can load an unsafe object to fit into your model. This issue is patched in version 5.0.13 with some basic fixes to avoid this, but is not 100% guaranteed when using `Object` type. The next major version will contain an allow-list to select what kind of Assembly can be loaded. Workarounds are detailed in the vendor advisory.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3884	Incorrect Default Permissions vulnerability in Hitachi Ops Center Analyzer on Windows (Hitachi Ops Center Analyzer RAID Agent component) allows local users to read and write specific files.This issue affects Hitachi Ops Center Analyzer: from 10.9.0-00 before 10.9.0-01.	7.3	More Details
CVE-2023-0997	A vulnerability was found in SourceCodester Moosikay E-Commerce System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /Moosikay/order.php of the component POST Parameter Handler. The manipulation of the argument username 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-221732.	7.3	More Details
CVE-2023-1039	A vulnerability classified as critical was found in SourceCodester Class and Exam Timetabling System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/index3.php of the component POST Parameter Handler. The manipulation of the argument password 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-221797 was assigned to this vulnerability.	7.3	More Details
CVE-2023-1037	A vulnerability was found in SourceCodester Dental Clinic Appointment Reservation System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /APR/login.php of the component POST Parameter Handler. The manipulation of the argument username 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-221795.	7.3	More Details
CVE-2023-25807	DataEase is an open source data visualization and analysis tool. When saving a dashboard on the DataEase platform saved data can be modified and store malicious code. This vulnerability can lead to the execution of malicious code stored by the attacker on the server side when the user accesses the dashboard. The vulnerability has been fixed in version 1.18.3.	7.2	More Details
CVE-2021-35290	File Upload vulnerability in balerocms-src 0.8.3 allows remote attackers to run arbitrary code via rich text editor on /admin/main/mod-blog page.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26035	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 are vulnerable to Unauthenticated Remote Code Execution via Missing Authorization. There are no permissions check on the snapshot action, which expects an id to fetch an existing monitor but can be passed an object to create a new one instead. TriggerOn ends up calling shell_exec using the supplied Id. This issue is fixed in This issue is fixed in versions 1.36.33 and 1.37.33.	7.2	More Details
CVE-2023-24249	An arbitrary file upload vulnerability in laravel-admin v1.8.19 allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details
CVE-2023-0278	The GeoDirectory WordPress plugin before 2.2.24 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin.	7.2	More Details
CVE-2023-0279	The Media Library Assistant WordPress plugin before 3.06 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin.	7.2	More Details
CVE-2023-20858	VMware Carbon Black App Control 8.7.x prior to 8.7.8, 8.8.x prior to 8.8.6, and 8.9.x.prior to 8.9.4 contain an injection vulnerability. A malicious actor with privileged access to the App Control administration console may be able to use specially crafted input allowing access to the underlying server operating system.	7.2	More Details
CVE-2023-0487	The My Sticky Elements WordPress plugin before 2.0.9 does not properly sanitise and escape a parameter before using it in a SQL statement when deleting messages, leading to a SQL injection exploitable by high privilege users such as admin	7.2	More Details
CVE-2023-27320	Sudo before 1.9.13p2 has a double free in the per-command chroot feature.	7.2	More Details
CVE-2023-26609	ABUS TVIP 20000-21150 devices allows remote attackers to execute arbitrary code via shell metacharacters in the /cgi-bin/mft/wireless_mft ap field.	7.2	More Details
CVE-2023-25432	An issue was discovered in Online Reviewer Management System v1.0. There is a SQL injection that can directly issue instructions to the background database system via reviewer_0/admins/assessments/course/course-update.php.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1070	External Control of File Name or Path in GitHub repository nilsteampassnet/teampass prior to 3.0.0.22.	7.1	More Details
CVE-2023-25154	Misskey is an open source, decentralized social media platform. In versions prior to 13.5.0 the link to the instance to the sender that appears when viewing a user or note received through ActivityPub is not properly validated, so by inserting a URL with a javascript scheme an attacker may execute JavaScript code in the context of the recipient. This issue has been fixed in version 13.5.0. Users are advised to upgrade. Users unable to upgrade should not "view on remote" for untrusted instances.	7.1	More Details
CVE-2023-26039	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain an OS Command Injection via daemonControl() in (/web/api/app/Controller/HostController.php). Any authenticated user can construct an api command to execute any shell command as the web user. This issue is patched in versions 1.36.33 and 1.37.33.	7.1	More Details
CVE-2023-24810	Misskey is an open source, decentralized social media platform. Due to insufficient validation of the redirect URL during `miauth` authentication in Misskey, arbitrary JavaScript can be executed when a user allows the link. All versions below 13.3.1 (including 12.x) are affected. This has been fixed in version 13.3.1. Users are advised to upgrade. Users unable to upgrade should not allow authentication of untrusted apps.	7.1	More Details
CVE-2023-24811	Misskey is an open source, decentralized social media platform. In versions prior to 13.3.2 the URL preview function is subject to a cross site scripting vulnerability due to insufficient URL validation. Arbitrary JavaScript is executed when a malicious URL is loaded in the `View in Player` or `View in Window` preview. This has been fixed in version 13.3.2. Users are advised to upgrade. Users unable to upgrade should avoid usage of the `View in Player` or `View in Window` functions.	7.1	More Details
CVE-2023-26607	In the Linux kernel 6.0.8, there is an out-of-bounds read in ntfs_attr_find in fs/ntfs/attrib.c.	7.1	More Details
CVE-2023-24419	Cross-Site Request Forgery (CSRF) vulnerability in Strategy11 Form Builder Team Formidable Forms plugin <= 5.5.6 versions.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27264	A missing permissions check in Mattermost Playbooks in Mattermost allows an attacker to modify a playbook via the /plugins/playbooks/api/v0/playbooks/[playbookID] API.	7.1	More Details
CVE-2023-22636	An unauthorized configuration download vulnerability in FortiWeb 6.3.6 through 6.3.21, 6.4.0 through 6.4.2 and 7.0.0 through 7.0.4 may allow a local attacker to access confidential configuration files via a crafted http request.	7.0	More Details
CVE-2023-0815	Potential Insertion of Sensitive Information into Jetty Log Files in multiple versions of OpenNMS Meridian and Horizon could allow disclosure of usernames and passwords if the logging level is set to debug. Users should upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet.	6.8	More Details
CVE-2023-20857	VMware Workspace ONE Content contains a passcode bypass vulnerability. A malicious actor, with access to a users rooted device, may be able to bypass the VMware Workspace ONE Content passcode.	6.8	More Details
CVE-2023-0846	Unauthenticated, stored cross-site scripting in the display of alarm reduction keys in multiple versions of OpenNMS Horizon and Meridian could allow an attacker access to confidential session information. Users should upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet.	6.7	More Details
CVE-2022-20551	In createTrack of AudioFlinger.cpp, there is a possible way to record audio without a privacy indicator due to a logic error in the code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-243376549	6.7	More Details
CVE-2023-0868	Reflected cross-site scripting in graph results in multiple versions of OpenNMS Meridian and Horizon could allow an attacker access to steal session cookies. Users should upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0867	Multiple stored and reflected cross-site scripting vulnerabilities in webapp jsp pages in multiple versions of OpenNMS Meridian and Horizon could allow an attacker access to confidential session information. Users should upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet.	6.7	More Details
CVE-2020-36652	Incorrect Default Permissions vulnerability in Hitachi Automation Director on Linux, Hitachi Infrastructure Analytics Advisor on Linux (Hitachi Infrastructure Analytics Advisor, Analytics probe server components), Hitachi Ops Center Automator on Linux, Hitachi Ops Center Analyzer on Linux (Hitachi Ops Center Analyzer, Analyzer probe server components), Hitachi Ops Center Viewpoint on Linux (Viewpoint RAID Agent component) allows local users to read and write specific files. This issue affects Hitachi Automation Director: from 8.2.0-00 through 10.6.1-00; Hitachi Infrastructure Analytics Advisor: from 2.0.0-00 through 4.0.0-00; Hitachi Ops Center Automator: before 10.9.1-00; Hitachi Ops Center Analyzer: before 10.9.1-00; Hitachi Ops Center Viewpoint: before 10.9.1-00.	6.6	More Details
CVE-2023-23296	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault.	6.5	More Details
CVE-2023-23916	An allocation of resources without limits or throttling vulnerability exists in curl <v7.88.0 based on the "chained" HTTP compression algorithms, meaning that a server response can be compressed multiple times and potentially with differentalgorithms. The number of acceptable "links" in this "decompression chain" wascapped, but the cap was implemented on a per-header basis allowing a maliciousserver to insert a virtually unlimited number of compression steps simply byusing many headers. The use of such a decompression chain could result in a "malloc bomb", making curl end up spending enormous amounts of allocated heap memory, or trying to and returning out of memory errors.	6.5	More Details
CVE-2022-23240	Active IQ Unified Manager for VMware vSphere, Linux, and Microsoft Windows versions prior to 9.11P1 are susceptible to a vulnerability which allows unauthorized users to update EMS Subscriptions via unspecified vectors.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23915	A cleartext transmission of sensitive information vulnerability exists in curl <v7.88.0 that could cause HSTS functionality to behave incorrectly when multiple URLs are requested in parallel. Using its HSTS support, curl can be instructed to use HTTPS instead of using an insecure clear-text HTTP step even when HTTP is provided in the URL. This HSTS mechanism would however surprisingly fail when multiple transfers are done in parallel as the HSTS cache file gets overwritten by the most recentlycompleted transfer. A later HTTP-only transfer to the earlier host name would then *not* get upgraded properly to HSTS.	6.5	More Details
CVE-2023-25621	Privilege Escalation vulnerability in Apache Software Foundation Apache Sling. Any content author is able to create i18n dictionaries in the repository in a location the author has write access to. As these translations are used across the whole product, it allows an author to change any text or dialog in the product. For example an attacker might fool someone by changing the text on a delete button to "Info". This issue affects the i18n module of Apache Sling up to version 2.5.18. Version 2.6.2 and higher limit by default i18m dictionaries to certain paths in the repository (/libs and /apps). Users of the module are advised to update to version 2.6.2 or higher, check the configuration for resource loading and then adjust the access permissions for the configured path accordingly.	6.5	More Details
CVE-2023-0998	A vulnerability classified as critical has been found in SourceCodester Alphaware Simple E-Commerce System 1.0. This affects an unknown part of the file /alphaware/summary.php of the component Payment Handler. The manipulation of the argument amount leads to improper access controls. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-221733 was assigned to this vulnerability.	6.5	More Details
CVE-2022-32784	The issue was addressed with improved UI handling. This issue is fixed in Safari 15.6, iOS 15.6 and iPadOS 15.6. Visiting a maliciously crafted website may leak sensitive data.	6.5	More Details
CVE-2023-1009	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical has been found in DrayTek Vigor 2960 1.5.1.4/1.5.1.5. Affected is the function sub_1DF14 of the file /cgi-bin/mainfunction.cgi of the component Web Management Interface. The manipulation of the argument option with the input /../etc/passwd- leads to path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-221742 is the identifier assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35369	Arbitrary File Read vulnerability found in Peacexie ImCat v.5.2 fixed in v.5.4 allows attackers to obtain sensitive information via the filtering_get_contents function.	6.5	More Details
CVE-2023-1065	This vulnerability in the Snyk Kubernetes Monitor can result in irrelevant data being posted to a Snyk Organization, which could in turn obfuscate other, relevant, security issues. It does not expose the user of the integration to any direct security risk and no user data can be leaked. To exploit the vulnerability the attacker does not need to be authenticated to Snyk but does need to know the target's Integration ID (which may or may not be the same as the Organization ID, although this is an unpredictable UUID in either case).	6.5	More Details
CVE-2022-31405	MV iDigital Clinic Enterprise (iDCE) 1.0 stores passwords in cleartext.	6.5	More Details
CVE-2022-40237	IBM MQ for HPE NonStop 8.1.0 is vulnerable to a denial of service attack due to an error within the CCDT and channel synchronization logic. IBM X-Force ID: 235727.	6.5	More Details
CVE-2023-26043	GeoNode is an open source platform that facilitates the creation, sharing, and collaborative use of geospatial data. GeoNode is vulnerable to an XML External Entity (XXE) injection in the style upload functionality of GeoServer leading to Arbitrary File Read. This issue has been patched in version 4.0.3.	6.5	More Details
CVE-2022-43870	IBM Spectrum Virtualize 8.3, 8.4, and 8.5 could disclose SNMPv3 server credentials to an authenticated user in log files. IBM X-Force ID: 239540.	6.5	More Details
CVE-2023-23512	The issue was addressed with improved handling of caches. This issue is fixed in watchOS 9.3, tvOS 16.3, macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. Visiting a website may lead to an app denial-of-service.	6.5	More Details
CVE-2023-0586	The All in One SEO Pack plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple parameters in versions up to, and including, 4.2.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with Contributor+ role to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0981	A vulnerability was found in SourceCodester Yoga Class Registration System 1.0. It has been classified as critical. Affected is an unknown function of the component Delete User. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-221676.	6.3	More Details
CVE-2023-0962	A vulnerability was found in SourceCodester Music Gallery Site 1.0. It has been declared as critical. This vulnerability affects unknown code of the file Master.php of the component GET Request Handler. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221632.	6.3	More Details
CVE-2023-1061	A vulnerability, which was classified as critical, has been found in SourceCodester Doctors Appointment System 1.0. This issue affects some unknown processing of the file /admin/edit-doc.php. The manipulation of the argument oldmail 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-221825 was assigned to this vulnerability.	6.3	More Details
CVE-2023-1100	A vulnerability classified as critical has been found in SourceCodester Online Catering Reservation System 1.0. This affects an unknown part of the file /reservation/add_message.php of the component POST Parameter Handler. The manipulation of the argument fullname 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 associated identifier of this vulnerability is VDB-222003.	6.3	More Details
CVE-2023-0961	A vulnerability was found in SourceCodester Music Gallery Site 1.0. It has been classified as critical. This affects an unknown part of the file view_music_details.php of the component GET Request Handler. 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 associated identifier of this vulnerability is VDB-221631.	6.3	More Details
CVE-2023-1038	A vulnerability classified as critical has been found in SourceCodester Online Reviewer Management System 1.0. Affected is an unknown function of the file /reviewer_0/admins/assessments/pretest/questions-view.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221796.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43873	An authenticated user can exploit a vulnerability in the IBM Spectrum Virtualize 8.2, 8.3, 8.4, and 8.5 GUI to execute code and escalate their privilege on the system. IBM X-Force ID: 239847.	6.3	More Details
CVE-2023-1059	A vulnerability classified as critical was found in SourceCodester Doctors Appointment System 1.0. This vulnerability affects unknown code of the file /admin/doctors.php of the component Parameter Handler. The manipulation of the argument search leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221824.	6.3	More Details
CVE-2023-0982	A vulnerability was found in SourceCodester Yoga Class Registration System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Add Class Entry. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The identifier VDB-221677 was assigned to this vulnerability.	6.3	More Details
CVE-2023-1099	A vulnerability was found in SourceCodester Online Student Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file eduauth/edit-class-detail.php. The manipulation of the argument editid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-222002 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-1062	A vulnerability, which was classified as critical, was found in SourceCodester Doctors Appointment System 1.0. Affected is an unknown function of the file /admin/add-new.php of the component Parameter Handler. The manipulation of the argument email leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-221826 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-1046	A vulnerability classified as critical has been found in MuYuCMS 2.2. This affects an unknown part of the file /admin.php/update/getFile.html. The manipulation of the argument url leads to server-side request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-221805 was assigned to this vulnerability.	6.3	More Details
CVE-2022-32844	A race condition was addressed with improved state handling. This issue is fixed in tvOS 15.6, watchOS 8.7, iOS 15.6 and iPadOS 15.6. An app with arbitrary kernel read and write capability may be able to bypass Pointer Authentication.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1063	A vulnerability has been found in SourceCodester Doctors Appointment System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/patient.php of the component Parameter Handler. The manipulation of the argument search 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-221827.	6.3	More Details
CVE-2023-1040	A vulnerability, which was classified as critical, has been found in SourceCodester Online Graduate Tracer System 1.0. Affected by this issue is some unknown functionality of the file tracking/admin/add_acc.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. VDB-221798 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-0986	A vulnerability classified as critical has been found in SourceCodester Sales Tracker Management System 1.0. This affects an unknown part of the file admin/?page=user/manage_user of the component Edit User. 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-221679.	6.3	More Details
CVE-2023-0980	A vulnerability was found in SourceCodester Yoga Class Registration System 1.0 and classified as critical. This issue affects some unknown processing of the file admin/registrations/update_status.php of the component Status Update Handler. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-221675.	6.3	More Details
CVE-2023-20016	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1056	A vulnerability was found in SourceCodester Doctors Appointment System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /edoc/doctor/patient.php. The manipulation of the argument search12 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-221821 was assigned to this vulnerability.	6.3	More Details
CVE-2023-1035	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been classified as critical. Affected is an unknown function of the file update_user.php. The manipulation of the argument user_id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221784.	6.3	More Details
CVE-2022-43923	IBM Maximo Application Suite 8.8.0 and 8.9.0 stores potentially sensitive information that could be read by a local user. IBM X-Force ID: 241584.	6.2	More Details
CVE-2021-22283	Improper Initialization vulnerability in ABB Relion protection relays - 611 series, ABB Relion protection relays - 615 series IEC 4.0 FP1, ABB Relion protection relays - 615 series CN 4.0 FP1, ABB Relion protection relays - 615 series IEC 5.0, ABB Relion protection relays - 615 series IEC 5.0 FP1, ABB Relion protection relays - 620 series IEC/CN 2.0, ABB Relion protection relays - 620 series IEC/CN 2.0 FP1, ABB Relion protection relays - REX640 PCL1, ABB Relion protection relays - REX640 PCL2, ABB Relion protection relays - REX640 PCL3, ABB Relion protection relays - RER615, ABB Remote Monitoring and Control - REC615, ABB Merging Unit- SMU615 allows Communication Channel Manipulation.This issue affects Relion protection relays - 611 series: from 1.0.0 before 2.0.3; Relion protection relays - 615 series IEC 4.0 FP1: from 4.1.0 before 4.1.9; Relion protection relays - 615 series CN 4.0 FP1: from 4.1.0 before 4.1.8; Relion protection relays - 615 series IEC 5.0: from 5.0.0 before 5.0.12; Relion protection relays - 615 series IEC 5.0 FP1: from 5.1.0 before 5.1.20; Relion protection relays - 620 series IEC/CN 2.0: from 2.0.0 before 2.0.11; Relion protection relays - 620 series IEC/CN 2.0 FP1: from 2.1.0 before 2.1.15; Relion protection relays - REX640 PCL1: from 1.0.0 before 1.0.8; Relion protection relays - REX640 PCL2: from 1.1.0 before 1.1.4; Relion protection relays - REX640 PCL3: from 1.2.0 before 1.2.1; Relion protection relays - RER615: from 2.0.0 before 2.0.3; Remote Monitoring and Control - REC615: from 1.0.0 before 2.0.3; Merging Unit- SMU615: from 1.0.0 before 1.0.2.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46784	SquaredUp Dashboard Server SCOM edition before 5.7.1 GA allows open redirection. (The issue was originally found in 5.5.1 GA.)	6.1	More Details
CVE-2022-46785	SquaredUp Dashboard Server SCOM edition before 5.7.1 GA allows XSS (issue 1 of 2).	6.1	More Details
CVE-2021-32302	Cross Site Scripting vulnerability in IRZ Electronics RUH2 GSM router allows attacker to obtain sensitive information via the Upload File parameter.	6.1	More Details
CVE-2022-45137	The configuration backend of the web-based management is vulnerable to reflected XSS (Cross-Site Scripting) attacks that targets the users browser. This leads to a limited impact of confidentiality and integrity but no impact of availability.	6.1	More Details
CVE-2023-26091	The frp_form_answers (aka Forms Export) extension before 3.1.2, and 4.x before 4.0.2, for TYPO3 allows XSS via saved emails.	6.1	More Details
CVE-2023-26042	Part-DB is an open source inventory management system for your electronic components. User input was found not being properly escaped, which allowed malicious users to inject arbitrary HTML into the pages. The Content-Security-Policy forbids inline and external scripts so it is not possible to execute JavaScript code, unless in combination with other vulnerabilities. There are no workarounds, please upgrade to Pat-DB 1.0.2 or later.	6.1	More Details
CVE-2022-38779	An open redirect issue was discovered in Kibana that could lead to a user being redirected to an arbitrary website if they use a maliciously crafted Kibana URL.	6.1	More Details
CVE-2022-48345	sanitize-url (aka @braintree/sanitize-url) before 6.0.2 allows XSS via HTML entities.	6.1	More Details
CVE-2022-29273	pfSense CE through 2.6.0 and pfSense Plus before 22.05 allow XSS in the WebGUI via URL Table Alias URL parameters.	6.1	More Details
CVE-2023-0044	If the Quarkus Form Authentication session cookie Path attribute is set to `/` then a cross-site attack may be initiated which might lead to the Information Disclosure. This attack can be prevented with the Quarkus CSRF Prevention feature.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0334	The ShortPixel Adaptive Images WordPress plugin before 3.6.3 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against any high privilege users such as admin	6.1	More Details
CVE-2023-1080	The GN Publisher plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in versions up to, and including, 1.5.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2022-32891	The issue was addressed with improved UI handling. This issue is fixed in Safari 16, tvOS 16, watchOS 9, iOS 16. Visiting a website that frames malicious content may lead to UI spoofing.	6.1	More Details
CVE-2023-27293	Improper neutralization of input during web page generation allows an unauthenticated attacker to submit malicious Javascript as the answer to a questionnaire which would then be executed when an authenticated user reviews the candidate's submission. This could be used to steal other users' cookies and force users to make actions without their knowledge.	6.1	More Details
CVE-2023-0043	The Custom Add User WordPress plugin through 2.0.2 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-25579	Nextcloud server is a self hosted home cloud product. In affected versions the `OC\Files\Node\Folder::getFullPath()` function was validating and normalizing the string in the wrong order. The function is used in the `newFile()` and `newFolder()` items, which may allow to creation of paths outside of ones own space and overwriting data from other users with crafted paths. This issue has been addressed in versions 25.0.2, 24.0.8, and 23.0.12. Users are advised to upgrade. There are no known workarounds for this issue.	6.0	More Details
CVE-2023-25540	Dell PowerScale OneFS 9.4.0.x contains an incorrect default permissions vulnerability. A local malicious user could potentially exploit this vulnerability to overwrite arbitrary files causing denial of service.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20015	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges.	6.0	More Details
CVE-2023-23520	A race condition was addressed with additional validation. This issue is fixed in watchOS 9.3, tvOS 16.3, macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. A user may be able to read arbitrary files as root.	5.9	More Details
CVE-2021-46841	This issue was addressed by using HTTPS when sending information over the network. This issue is fixed in Apple Music 3.5.0 for Android. An attacker in a privileged network position can track a user's activity.	5.9	More Details
CVE-2023-27371	GNU libmicrohttpd before 0.9.76 allows remote DoS (Denial of Service) due to improper parsing of a multipart/form-data boundary in the postprocessor.c MHD_create_post_processor() method. This allows an attacker to remotely send a malicious HTTP POST packet that includes one or more '\0' bytes in a multipart/form-data boundary field, which - assuming a specific heap layout - will result in an out-of-bounds read and a crash in the find_boundary() function.	5.9	More Details
CVE-2023-0869	Cross-site scripting in outage/list.htm in multiple versions of OpenNMS Meridian and Horizon allows an attacker access to confidential session information. The solution is to upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4 or newer. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet.	5.8	More Details
CVE-2023-23039	An issue was discovered in the Linux kernel through 6.2.0-rc2. drivers/tty/vcc.c has a race condition and resultant use-after-free if a physically proximate attacker removes a VCC device while calling open(), aka a race condition between vcc_open() and vcc_remove().	5.7	More Details
CVE-2023-25821	Nextcloud is an Open Source private cloud software. Versions 24.0.4 and above, prior to 24.0.7, and 25.0.0 and above, prior to 25.0.1, contain Improper Access Control. Secure view for internal shares can be circumvented if reshare permissions are also given. This issue is patched in versions 24.0.7 and 25.0.1. No workaround is available.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23501	The issue was addressed with improved memory handling This issue is fixed in macOS Ventura 13.2. An app may be able to disclose kernel memory.	5.5	More Details
CVE-2023-23502	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in macOS Monterey 12.6.3, macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3, tvOS 16.3, watchOS 9.3. An app may be able to determine kernel memory layout.	5.5	More Details
CVE-2023-23503	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3. An app may be able to bypass Privacy preferences.	5.5	More Details
CVE-2023-22998	In the Linux kernel before 6.0.3, drivers/gpu/drm/virtio/virtgpu_object.c misinterprets the drm_gem_shmem_get_sg_table return value (expects it to be NULL in the error case, whereas it is actually an error pointer).	5.5	More Details
CVE-2023-22997	In the Linux kernel before 6.1.2, kernel/module/decompress.c misinterprets the module_get_next_page return value (expects it to be NULL in the error case, whereas it is actually an error pointer).	5.5	More Details
CVE-2023-23508	The issue was addressed with improved memory handling. This issue is fixed in macOS Big Sur 11.7.3, macOS Ventura 13.2, macOS Monterey 12.6.3. An app may be able to bypass Privacy preferences.	5.5	More Details
CVE-2023-23510	A permissions issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.2. An app may be able to access a user's Safari history.	5.5	More Details
CVE-2022-48305	There is an identity authentication bypass vulnerability in Huawei Children Smart Watch (Simba-AL00) 1.1.1.274. Successful exploitation of this vulnerability may cause the access control function of specific applications to fail.	5.5	More Details
CVE-2022-20481	In multiple files, there is a possible way to preserve WiFi settings due to residual data after a reset. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-241927115	5.5	More Details
CVE-2022-22582	A validation issue existed in the handling of symlinks. This issue was addressed with improved validation of symlinks. This issue is fixed in Security Update 2022-003 Catalina, macOS Big Sur 11.6.5, macOS Monterey 12.3. A local user may be able to write arbitrary files.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22668	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3. A malicious application may be able to leak sensitive user information.	5.5	More Details
CVE-2022-20455	In addAutomaticZenRule of ZenModeHelper.java, there is a possible persistent denial of service due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242537431	5.5	More Details
CVE-2022-32824	The issue was addressed with improved memory handling. This issue is fixed in tvOS 15.6, watchOS 8.7, iOS 15.6 and iPadOS 15.6. An app may be able to disclose kernel memory.	5.5	More Details
CVE-2022-32855	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.6 and iPadOS 15.6. A user may be able to view restricted content from the lock screen.	5.5	More Details
CVE-2022-32896	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Monterey 12.6, macOS Big Sur 11.7. A user may be able to view sensitive user information.	5.5	More Details
CVE-2022-32902	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13, macOS Monterey 12.6, macOS Big Sur 11.7. An app may be able to bypass Privacy preferences.	5.5	More Details
CVE-2023-1055	A flaw was found in RHDS 11 and RHDS 12. While browsing entries LDAP tries to decode the userPassword attribute instead of the userCertificate attribute which could lead into sensitive information leaked. An attacker with a local account where the cockpit-389-ds is running can list the processes and display the hashed passwords. The highest threat from this vulnerability is to data confidentiality.	5.5	More Details
CVE-2023-23522	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Ventura 13.2.1. An app may be able to observe unprotected user data.	5.5	More Details
CVE-2022-41727	An attacker can craft a malformed TIFF image which will consume a significant amount of memory when passed to DecodeConfig. This could lead to a denial of service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1018	An out-of-bounds read vulnerability exists in TPM2.0's Module Library allowing a 2-byte read past the end of a TPM2.0 command in the CryptParameterDecryption routine. An attacker who can successfully exploit this vulnerability can read or access sensitive data stored in the TPM.	5.5	More Details
CVE-2023-1057	A vulnerability was found in SourceCodester Doctors Appointment System 1.0. It has been rated as critical. Affected by this issue is the function edoc of the file login.php. The manipulation of the argument usermail leads to sql injection. VDB-221822 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2023-23511	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.6.3, macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3, tvOS 16.3, watchOS 9.3. An app may be able to bypass Privacy preferences.	5.5	More Details
CVE-2023-23500	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3. An app may be able to leak sensitive kernel state.	5.5	More Details
CVE-2023-23506	A permissions issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.2. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2023-23499	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Monterey 12.6.3, macOS Ventura 13.2, watchOS 9.3, macOS Big Sur 11.7.3, tvOS 16.3, iOS 16.3 and iPadOS 16.3. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2023-22996	In the Linux kernel before 5.17.2, drivers/soc/qcom/qcom_aoss.c does not release an of_find_device_by_node reference after use, e.g., with put_device.	5.5	More Details
CVE-2021-33367	Buffer Overflow vulnerability in Freeimage v3.18.0 allows attacker to cause a denial of service via a crafted JXR file.	5.5	More Details
CVE-2022-46704	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.1, macOS Big Sur 11.7.2, macOS Monterey 12.6.2. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2023-23205	An issue was discovered in lib60870 v2.3.2. There is a memory leak in lib60870/lib60870-C/examples/multi_client_server/multi_client_server.c.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1095	In nf_tables_updtable, if nf_tables_table_enable returns an error, nft_trans_destroy is called to free the transaction object. nft_trans_destroy() calls list_del(), but the transaction was never placed on a list -- the list head is all zeroes, this results in a NULL pointer dereference.	5.5	More Details
CVE-2023-0597	A flaw possibility of memory leak in the Linux kernel cpu_entry_area mapping of X86 CPU data to memory was found in the way user can guess location of exception stack(s) or other important data. A local user could use this flaw to get access to some important data with expected location in memory.	5.5	More Details
CVE-2022-46440	ttftool v0.9.2 was discovered to contain a segmentation violation via the readU16 function at ttf.c.	5.5	More Details
CVE-2023-22999	In the Linux kernel before 5.16.3, drivers/usb/dwc3/dwc3-qcom.c misinterprets the dwc3_qcom_create_urs_usb_platdev return value (expects it to be NULL in the error case, whereas it is actually an error pointer).	5.5	More Details
CVE-2023-1008	A vulnerability was found in Twister Antivirus 8.17. It has been rated as problematic. This issue affects the function 0x801120E4 in the library filmfd.sys of the component IoControlCode Handler. The manipulation leads to denial of service. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The identifier VDB-221741 was assigned to this vulnerability.	5.5	More Details
CVE-2022-4788	The Embed PDF WordPress plugin through 1.0.6 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2022-4829	The Show-Hide / Collapse-Expand WordPress plugin before 1.3.0 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.	5.4	More Details
CVE-2022-4757	The List Pages Shortcode WordPress plugin before 1.7.6 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0539	The GS Insever Portfolio WordPress plugin before 1.4.5 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2023-0168	The Olevmedia Shortcodes WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2022-4679	The Wufoo Shortcode WordPress plugin before 1.52 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2023-0230	The VK All in One Expansion Unit WordPress plugin before 9.86.0.0 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2023-27295	Cross-site request forgery is facilitated by OpenCATS failure to require CSRF tokens in POST requests. An attacker can exploit this issue by creating a dummy page that executes Javascript in an authenticated user's session when visited.	5.4	More Details
CVE-2023-1022	The WP Meta SEO plugin for WordPress is vulnerable to unauthorized options update due to a missing capability check on the wpmsGGSaveInformation function in versions up to, and including, 4.5.3. This makes it possible for authenticated attackers with subscriber-level access to update google analytics options maintained by the plugin. This vulnerability occurred as a result of the plugin relying on nonce checks as a means of access control, and that nonce being accessible to all authenticated users regardless of role.	5.4	More Details
CVE-2023-1023	The WP Meta SEO plugin for WordPress is vulnerable to unauthorized plugin settings update due to a missing capability check on the saveSitemapSettings function in versions up to, and including, 4.5.3. This makes it possible for authenticated attackers with subscriber-level access to change sitemap-related settings of the plugin. This vulnerability occurred as a result of the plugin relying on nonce checks as a means of access control, and that nonce being accessible to all authenticated users regardless of role.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0535	The Donation Block For PayPal WordPress plugin before 2.1.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2023-23158	A stored cross-site scripting (XSS) vulnerability in Art Gallery Management System Project v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the message parameter on the enquiry page.	5.4	More Details
CVE-2023-0552	The Registration Forms WordPress plugin before 3.8.2.3 does not properly validate the redirection URL when logging in and login out, leading to an Open Redirect vulnerability	5.4	More Details
CVE-2023-23157	A stored cross-site scripting (XSS) vulnerability in Art Gallery Management System Project v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the fullname parameter on the enquiry page.	5.4	More Details
CVE-2023-22860	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244100.	5.4	More Details
CVE-2023-24251	WangEditor v5 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /dist/index.js.	5.4	More Details
CVE-2023-24651	Simple Customer Relationship Management System v1.0 was discovered to contain a SQL injection vulnerability via the name parameter on the registration page.	5.4	More Details
CVE-2022-43459	Cross-Site Request Forgery (CSRF) vulnerability in Forms by CaptainForm – Form Builder for WordPress plugin <= 2.5.3 versions.	5.4	More Details
CVE-2023-23992	Cross-Site Request Forgery (CSRF) vulnerability in AutomatorWP plugin <= 2.5.0 leads to object delete.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27294	Improper neutralization of input during web page generation allows an authenticated attacker with access to a restricted account to submit malicious Javascript as the description for a calendar event, which would then be executed in other users' browsers if they browse to that event. This could result in stealing session tokens from users with higher permission levels or forcing users to make actions without their knowledge.	5.4	More Details
CVE-2023-23983	Cross-Site Request Forgery (CSRF) vulnerability in wpdevart Responsive Vertical Icon Menu plugin <= 1.5.8 can lead to theme deletion.	5.4	More Details
CVE-2023-22425	Stored cross-site scripting vulnerability in Schedule function of SHIRASAGI v1.16.2 and earlier versions allows a remote authenticated attacker to inject an arbitrary script.	5.4	More Details
CVE-2023-0995	Cross-site Scripting (XSS) - Stored in GitHub repository unilogies/bumsys prior to v2.0.1.	5.4	More Details
CVE-2023-27292	An open redirect vulnerability exposes OpenCATS to template injection due to improper validation of user-supplied GET parameters.	5.4	More Details
CVE-2023-25823	Gradio is an open-source Python library to build machine learning and data science demos and web applications. Versions prior to 3.13.1 contain Use of Hard-coded Credentials. When using Gradio's share links (i.e. creating a Gradio app and then setting `share=True`), a private SSH key is sent to any user that connects to the Gradio machine, which means that a user could access other users' shared Gradio demos. From there, other exploits are possible depending on the level of access/exposure the Gradio app provides. This issue is patched in version 3.13.1, however, users are recommended to update to 3.19.1 or later where the FRP solution has been properly tested.	5.4	More Details
CVE-2022-46786	SquaredUp Dashboard Server SCOM edition before 5.7.1 GA allows XSS (issue 2 of 2).	5.4	More Details
CVE-2022-4795	The Galleries by Angie Makes WordPress plugin through 1.67 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48343	In JetBrains TeamCity before 2022.10.2 there was an XSS vulnerability in the user creation process.	5.4	More Details
CVE-2023-1067	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.18.	5.4	More Details
CVE-2023-26038	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain a Local File Inclusion (Untrusted Search Path) vulnerability via web/ajax/modal.php, where an arbitrary php file path can be passed in the request and loaded. This issue is patched in versions 1.36.33 and 1.37.33.	5.4	More Details
CVE-2022-48344	In JetBrains TeamCity before 2022.10.2 there was an XSS vulnerability in the group creation process.	5.4	More Details
CVE-2023-22972	A Reflected Cross-site scripting (XSS) vulnerability in interface/forms/eye_mag/php/eye_mag_functions.php in OpenEMR < 7.0.0 allows remote authenticated users to inject arbitrary web script or HTML via the REQUEST_URI.	5.4	More Details
CVE-2023-24415	Cross-Site Request Forgery (CSRF) vulnerability in QuantumCloud AI ChatBot plugin <= 4.2.8 versions.	5.4	More Details
CVE-2023-26103	Versions of the package deno before 1.31.0 are vulnerable to Regular Expression Denial of Service (ReDoS) due to the upgradeWebSocket function, which contains regexes in the form of /s*,s*/, used for splitting the Connection/Upgrade header. A specially crafted Connection/Upgrade header can be used to significantly slow down a web socket server.	5.3	More Details
CVE-2023-23689	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	5.3	More Details
CVE-2022-45139	A CORS Misconfiguration in the web-based management allows a malicious third party webserver to misuse all basic information pages on the webserver. In combination with CVE-2022-45138 this could lead to disclosure of device information like CPU diagnostics. As there is just a limited amount of information readable the impact only affects a small subset of confidentiality.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1007	A vulnerability was found in Twister Antivirus 8.17. It has been declared as critical. This vulnerability affects the function 0x801120E4 in the library filmfd.sys of the component IoControlCode Handler. The manipulation leads to improper access controls. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221740.	5.3	More Details
CVE-2022-32906	This issue was addressed with using HTTPS when sending information over the network. This issue is fixed in Apple Music 3.9.10 for Android. A user in a privileged network position may intercept SSL/TLS connections.	5.3	More Details
CVE-2023-1048	A vulnerability, which was classified as critical, has been found in TechPowerUp Ryzen DRAM Calculator 1.2.0.5. This issue affects some unknown processing in the library WinRing0x64.sys. The manipulation leads to improper initialization. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-221807.	5.3	More Details
CVE-2020-9846	A logic issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.0.1. A malicious application may be able to access local users' Apple IDs.	5.3	More Details
CVE-2023-1010	A vulnerability classified as critical was found in vox2png 1.0. Affected by this vulnerability is an unknown functionality of the file vox2png.c. The manipulation leads to heap-based buffer overflow. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-221743.	5.3	More Details
CVE-2023-1047	A vulnerability classified as critical was found in TechPowerUp RealTemp 3.7.0.0. This vulnerability affects unknown code in the library WinRing0x64.sys. The manipulation leads to improper initialization. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. VDB-221806 is the identifier assigned to this vulnerability.	5.3	More Details
CVE-2023-0595	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions)	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1005	A vulnerability was found in JP1016 Markdown-Electron and classified as critical. Affected by this issue is some unknown functionality. The manipulation leads to code injection. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. VDB-221738 is the identifier assigned to this vulnerability.	5.3	More Details
CVE-2023-1004	A vulnerability has been found in MarkText up to 0.17.1 on Windows and classified as critical. Affected by this vulnerability is an unknown functionality of the component WSH JScript Handler. The manipulation leads to code injection. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier VDB-221737 was assigned to this vulnerability.	5.3	More Details
CVE-2023-20012	A vulnerability in the CLI console login authentication of Cisco Nexus 9300-FX3 Series Fabric Extender (FEX) when used in UCS Fabric Interconnect deployments could allow an unauthenticated attacker with physical access to bypass authentication. This vulnerability is due to the improper implementation of the password validation function. An attacker could exploit this vulnerability by logging in to the console port on an affected device. A successful exploit could allow the attacker to bypass authentication and execute a limited set of commands local to the FEX, which could cause a device reboot and denial of service (DoS) condition.	5.3	More Details
CVE-2022-48342	In JetBrains TeamCity before 2022.10.2 jVMTI was enabled by default on agents.	5.2	More Details
CVE-2023-0964	A vulnerability classified as critical has been found in SourceCodester Sales Tracker Management System 1.0. Affected is an unknown function of the file admin/products/view_product.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. VDB-221634 is the identifier assigned to this vulnerability.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4203	A read buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. The read buffer overrun might result in a crash which could lead to a denial of service attack. In theory it could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext) although we are not aware of any working exploit leading to memory contents disclosure as of the time of release of this advisory. In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects.	4.9	More Details
CVE-2023-22427	Stored cross-site scripting vulnerability in Theme switching function of SHIRASAGI v1.16.2 and earlier versions allows a remote attacker with an administrative privilege to inject an arbitrary script.	4.8	More Details
CVE-2022-23239	Active IQ Unified Manager for VMware vSphere, Linux, and Microsoft Windows versions prior to 9.11P1 are susceptible to a vulnerability which allows administrative users to perform a Stored Cross-Site Scripting (XSS) attack.	4.8	More Details
CVE-2023-0543	The Arigato Autoresponder and Newsletter WordPress plugin before 2.1.7.2 does not sanitize and escape some of its settings, which could allow high-privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2023-0548	The Namaste! LMS WordPress plugin before 2.5.9.4 does not sanitize 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-2023-1081	Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 1.3.3.	4.8	More Details
CVE-2023-0949	Cross-site Scripting (XSS) - Reflected in GitHub repository modoboa/modoboa prior to 2.0.5.	4.8	More Details
CVE-2023-25431	An issue was discovered in Online Reviewer Management System v1.0. There is a XSS vulnerability via reviewer_0/admins/assessments/course/course-update.php.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26545	In the Linux kernel before 6.1.13, there is a double free in net/mpls/af_mpls.c upon an allocation failure (for registering the sysctl table under a new location) during the renaming of a device.	4.7	More Details
CVE-2023-0960	A vulnerability was found in SeaCMS 11.6 and classified as problematic. Affected by this issue is some unknown functionality of the file /data/config.ftp.php of the component Picture Management. The manipulation leads to deserialization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-221630 is the identifier assigned to this vulnerability.	4.7	More Details
CVE-2023-1054	A vulnerability was found in SourceCodester Music Gallery Site 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/?page=user/manage. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-221820.	4.7	More Details
CVE-2023-1053	A vulnerability was found in SourceCodester Music Gallery Site 1.0 and classified as critical. This issue affects some unknown processing of the file view_category.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-221819.	4.7	More Details
CVE-2022-46713	A race condition was addressed with additional validation. This issue is fixed in macOS Ventura 13, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. An app may be able to modify protected parts of the file system.	4.7	More Details
CVE-2022-1607	Cross-Site Request Forgery (CSRF) vulnerability in ABB Pulsar Plus System Controller NE843_S, ABB Infinity DC Power Plant allows Cross Site Request Forgery.This issue affects Pulsar Plus System Controller NE843_S : comcode 150042936; Infinity DC Power Plant: H5692448 G104 G842 G224L G630-4 G451C(2) G461(2) – comcode 150047415.	4.6	More Details
CVE-2022-48254	There is a data processing error vulnerability in Leia-B29 2.0.0.49(M03). Successful exploitation could bypass lock screen authentication.	4.6	More Details
CVE-2022-43578	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.7 and 6.1.0.0 through 6.1.2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 238683.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0585	The All in One SEO Pack plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple parameters in versions up to, and including, 4.2.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with Administrator role or above to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	4.4	More Details
CVE-2023-20050	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user.	4.4	More Details
CVE-2023-1028	The WP Meta SEO plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.5.3. This is due to missing or incorrect nonce validation on the setIgnore function. This makes it possible for unauthenticated attackers to update plugin options via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-27263	A missing permissions check in the /plugins/playbooks/api/v0/runs API in Mattermost allows an attacker to list and view playbooks belonging to a team they are not a member of.	4.3	More Details
CVE-2023-1068	The Download Read More Excerpt Link plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.6.0. This is due to missing or incorrect nonce validation on the read_more_excerpt_link_menu_options() function. This makes it possible for unauthenticated attackers to update he plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2022-46705	A spoofing issue existed in the handling of URLs. This issue was addressed with improved input validation. This issue is fixed in iOS 16.2 and iPadOS 16.2, macOS Ventura 13.1, Safari 16.2. Visiting a malicious website may lead to address bar spoofing.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1036	A vulnerability was found in SourceCodester Dental Clinic Appointment Reservation System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /APR/signup.php of the component POST Parameter Handler. The manipulation of the argument firstname leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-221794 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2023-1043	A vulnerability was found in MuYuCMS 2.2. It has been classified as problematic. Affected is an unknown function of the file /editor/index.php. The manipulation of the argument dir_path leads to relative path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-221802 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2023-1044	A vulnerability was found in MuYuCMS 2.2. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /editor/index.php. The manipulation of the argument file_path leads to relative path traversal. 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-221803.	4.3	More Details
CVE-2023-1029	The WP Meta SEO plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.5.3. This is due to missing or incorrect nonce validation on the regenerateSitemaps function. This makes it possible for unauthenticated attackers to regenerate Sitemaps via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-1002	A vulnerability, which was classified as problematic, has been found in MuYuCMS 2.2. This issue affects some unknown processing of the file index.php. The manipulation of the argument file_path leads to path traversal. 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-221735.	4.3	More Details
CVE-2023-0988	A vulnerability, which was classified as problematic, has been found in SourceCodester Online Pizza Ordering System 1.0. This issue affects some unknown processing of the file admin/ajax.php?action=save_user. The manipulation leads to cross-site request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-221681 was assigned to this vulnerability.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23865	Cross-Site Request Forgery (CSRF) vulnerability in Checkout Plugins Stripe Payments For WooCommerce plugin <= 1.4.10 leads to settings change.	4.3	More Details
CVE-2023-1024	The WP Meta SEO plugin for WordPress is vulnerable to unauthorized sitemap generation due to a missing capability check on the regenerateSitemaps function in versions up to, and including, 4.5.3. This makes it possible for authenticated attackers with subscriber-level access to generate sitemaps. This vulnerability occurred as a result of the plugin relying on nonce checks as a means of access control, and that nonce being accessible to all authenticated users regardless of role.	4.3	More Details
CVE-2023-1026	The WP Meta SEO plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the listPostsCategory function in versions up to, and including, 4.5.3. This makes it possible for authenticated attackers with subscriber-level access to get post listings by category as long as those posts are published. This vulnerability occurred as a result of the plugin relying on nonce checks as a means of access control, and that nonce being accessible to all authenticated users regardless of role.	4.3	More Details
CVE-2023-0999	A vulnerability classified as problematic was found in SourceCodester Sales Tracker Management System 1.0. This vulnerability affects unknown code of the file admin/?page=user/list. The manipulation leads to cross-site request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-221734 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2023-25816	Nextcloud is an Open Source private cloud software. Versions 25.0.0 and above, prior to 25.0.3, are subject to Uncontrolled Resource Consumption. A user can configure a very long password, consuming more resources on password validation than desired. This issue is patched in 25.0.3 No workaround is available.	4.3	More Details
CVE-2022-47612	Cross-Site Request Forgery (CSRF) vulnerability in Roland Barker, xnau webdesign Participants Database plugin <= 2.4.5 leads to list column update.	4.3	More Details
CVE-2022-47179	Cross-Site Request Forgery (CSRF) vulnerability in Uwe Jacobs OWM Weather plugin <= 5.6.11 leads to post duplication as a draft.	4.3	More Details
CVE-2023-23659	Cross-Site Request Forgery (CSRF) vulnerability in MainWP Matomo Extension <= 4.0.4 versions.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24384	Cross-Site Request Forgery (CSRF) vulnerability in WpDevArt Organization chart <= 1.4.4 versions.	4.3	More Details
CVE-2023-1027	The WP Meta SEO plugin for WordPress is vulnerable to unauthorized sitemap generation due to a missing capability check on the checkAllCategoryInSitemap function in versions up to, and including, 4.5.3. This makes it possible for authenticated attackers with subscriber-level access to obtain post categories. This vulnerability occurred as a result of the plugin relying on nonce checks as a means of access control, and that nonce being accessible to all authenticated users regardless of role.	4.3	More Details
CVE-2023-22476	Mantis Bug Tracker (MantisBT) is an open source issue tracker. In versions prior to 2.25.6, due to insufficient access-level checks, any logged-in user allowed to perform Group Actions can access to the _Summary_ field of private Issues (i.e. having Private view status, or belonging to a private Project) via a crafted `bug_arr[]` parameter in *bug_actiongroup_ext.php*. This issue is fixed in version 2.25.6. There are no workarounds.	4.3	More Details
CVE-2023-23920	An untrusted search path vulnerability exists in Node.js. <19.6.1, <18.14.1, <16.19.1, and <14.21.3 that could allow an attacker to search and potentially load ICU data when running with elevated privileges.	4.2	More Details
CVE-2022-34910	An issue was discovered in the A4N (Aremis 4 Nomad) application 1.5.0 for Android. It uses a local database to store data and accounts. However, the password is stored in cleartext. Therefore, an attacker can retrieve the passwords of other users that used the same device.	4.1	More Details
CVE-2023-1045	A vulnerability was found in MuYuCMS 2.2. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin.php/accessory/filesdel.html. The manipulation of the argument filedelur leads to relative path traversal. 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-221804.	3.8	More Details
CVE-2021-4325	A vulnerability, which was classified as problematic, has been found in NHN TOAST UI Chart 4.1.4. This issue affects some unknown processing of the component Legend Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. Upgrading to version 4.2.0 is able to address this issue. The identifier of the patch is 1a3f455d17df379e11b501bb5ba1dd1bcc41d63e. It is recommended to upgrade the affected component. The identifier VDB-221501 was assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1041	A vulnerability, which was classified as problematic, was found in SourceCodester Simple Responsive Tourism Website 1.0. This affects an unknown part of the file /tourism/rate_review.php. The manipulation of the argument id with the input 1"><script>alert(1111)</script> 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 associated identifier of this vulnerability is VDB-221799.	3.5	More Details
CVE-2019-25105	A vulnerability, which was classified as problematic, was found in dro.pm. This affects an unknown part of the file web/fileman.php. The manipulation of the argument secret/key leads to cross site scripting. 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 patch is named fa73c3a42bc5c246a1b8f815699ea241aef154bb. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-221763.	3.5	More Details
CVE-2023-1030	A vulnerability has been found in SourceCodester Online Boat Reservation System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /boat/login.php of the component POST Parameter Handler. The manipulation of the argument un leads to cross site scripting. 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-221755.	3.5	More Details
CVE-2023-1042	A vulnerability has been found in SourceCodester Online Pet Shop We App 1.0 and classified as problematic. This vulnerability affects unknown code of the file /pet_shop/admin/orders/update_status.php. The manipulation of the argument oid with the input 1"><script>alert(1111) </script> leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221800.	3.5	More Details
CVE-2023-1006	A vulnerability was found in SourceCodester Medical Certificate Generator App 1.0. It has been classified as problematic. This affects an unknown part of the component New Record Handler. The manipulation of the argument Firstname/Middlename/Lastname/Suffix/Nationality/Doctor Fullname/Doctor Suffix with the input "><script>prompt(1)</script> leads to cross site scripting. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-221739.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0987	A vulnerability classified as problematic was found in SourceCodester Online Pizza Ordering System 1.0. This vulnerability affects unknown code of the file index.php?page=checkout. 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. The identifier of this vulnerability is VDB-221680.	3.5	More Details
CVE-2022-42838	An issue with app access to camera data was addressed with improved logic. This issue is fixed in macOS Ventura 13. A camera extension may be able to continue receiving video after the app which activated was closed.	3.3	More Details
CVE-2023-0481	In RestEasy Reactive implementation of Quarkus the insecure File.createTempFile() is used in the FileBodyHandler class which creates temp files with insecure permissions that could be read by a local user.	3.3	More Details
CVE-2023-23493	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3. An encrypted volume may be unmounted and remounted by a different user without prompting for the password.	3.3	More Details
CVE-2023-23498	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.7.3 and iPadOS 15.7.3, macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. The quoted original message may be selected from the wrong email when forwarding an email from an Exchange account.	3.3	More Details
CVE-2023-26303	Denial of service could be caused to markdown-it-py, before v2.2.0, if an attacker was allowed to force null assertions with specially crafted input.	3.3	More Details
CVE-2023-26302	Denial of service could be caused to the command line interface of markdown-it-py, before v2.2.0, if an attacker was allowed to use invalid UTF-8 characters as input.	3.3	More Details
CVE-2023-23505	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Monterey 12.6.3, macOS Ventura 13.2, watchOS 9.3, macOS Big Sur 11.7.3, iOS 15.7.3 and iPadOS 15.7.3, iOS 16.3 and iPadOS 16.3. An app may be able to access information about a user’s contacts.	3.3	More Details
CVE-2022-3219	GnuPG can be made to spin on a relatively small input by (for example) crafting a public key with thousands of signatures attached, compressed down to just a few KB.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20932	In onCreatePreferences of EditInfoFragment.java, there is a possible way to read contacts belonging to other users due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-248251018	3.3	More Details
CVE-2023-27266	Mattermost fails to honor the ShowEmailAddress setting when constructing a response to the /api/v4/users/me/teams API endpoint, allowing an attacker with team admin privileges to learn the team owner's email address in the response.	2.7	More Details
CVE-2023-27265	Mattermost fails to honor the ShowEmailAddress setting when constructing a response to the "Regenerate Invite Id" API endpoint, allowing an attacker with team admin privileges to learn the team owner's email address in the response.	2.7	More Details
CVE-2023-26041	Nextcloud Talk is a fully on-premises audio/video and chat communication service. When cron jobs were misconfigured and therefore messages are not expired, the API would still return them while they were then hidden by the frontend code. It is recommended that the Nextcloud Talk is upgraded to 15.0.3. There are no workaround available.	2.6	More Details
CVE-2023-0966	A vulnerability classified as problematic was found in SourceCodester Online Eyewear Shop 1.0. Affected by this vulnerability is an unknown functionality of the file admin/?page=orders/view_order. The manipulation of the argument id leads to cross site scripting. 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-221635.	2.4	More Details
CVE-2019-0118	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2017-1004	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2019-11138	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-11134	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-11130	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-11122	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-0133	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-11118	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-0125	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-11116	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-11115	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2017-1005	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2019-11099	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-0176	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2017-1003	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2019-0100	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-1002	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2019-0137	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2017-1001	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1000	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-0999	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-0998	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-0997	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-0996	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2019-0156	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2017-0995	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-0994	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-0087	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-0095	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-0167	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2018-12164	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2017-1006	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1031	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1025	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1026	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1027	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1028	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1029	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1030	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-1032	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1023	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1033	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1034	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1035	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1036	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1037	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1038	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1024	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1022	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1007	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-1013	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2019-11142	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2017-1008	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1009	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1010	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1011	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1012	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1014	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1021	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1015	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1016	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-1017	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1018	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1019	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1020	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2019-11141	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-11144	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2017-1040	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2019-14635	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14643	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14642	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14641	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14640	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14639	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14638	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14637	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14636	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14634	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-11149	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14633	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14632	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14631	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14628	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14627	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14624	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14623	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14622	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14644	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14645	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14646	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14647	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2017-0981	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-0982	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-0983	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-0984	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-0985	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-0986	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-0987	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-0988	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-0989	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-0990	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-0991	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-0992	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-0993	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2019-14651	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14650	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14649	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14648	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14621	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14619	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14618	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14573	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14571	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14567	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14564	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14561	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14560	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14555	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14554	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14552	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-11183	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-11176	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-11169	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-11164	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-11161	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-11160	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-11159	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-11158	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-11150	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14572	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14576	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14617	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14577	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14616	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14614	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14606	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14597	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14595	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14594	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14593	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14592	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14589	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14588	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14585	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14583	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14582	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14581	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14580	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14579	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2019-14578	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none.	N/A	More Details
CVE-2017-1039	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1049	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1041	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2018-18138	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-18145	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18144	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18143	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18142	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18141	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18140	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18139	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18137	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18166	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18136	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18135	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18134	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-18133	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18132	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18131	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18130	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18146	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18147	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18148	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18149	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18164	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18163	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18162	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-18161	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18160	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18159	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18158	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18157	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18156	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18155	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18154	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18153	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18152	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18151	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18150	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-18129	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18128	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18127	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18108	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18106	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18105	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18104	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18103	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18102	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18101	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18100	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-18099	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18092	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-12197	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-12195	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-12194	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-12186	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-12184	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-12170	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18107	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18109	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18126	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-18110	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18125	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18124	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18123	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18122	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18121	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18120	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18119	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18118	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18117	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18116	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18115	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-18114	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18113	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18112	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18111	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18165	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18167	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2017-1042	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1069	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1062	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1063	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1064	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1065	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-1066	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1067	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1068	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2023-0884	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-3759. Reason: This candidate is a reservation duplicate of CVE-2022-3759. Notes: All CVE users should reference CVE-2022-3759 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2018-18168	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2023-0885	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-0518. Reason: This candidate is a reservation duplicate of CVE-2023-0518. Notes: All CVE users should reference CVE-2023-0518 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-0886	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-3411. Reason: This candidate is a reservation duplicate of CVE-2022-3411. Notes: All CVE users should reference CVE-2022-3411 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2021-45032	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2022-2176	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34064	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-33563. Reason: This candidate is a duplicate of CVE-2021-33563. Notes: All CVE users should reference CVE-2021-33563 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2021-34248	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-25905. Reason: This candidate is a duplicate of CVE-2020-25905. Notes: All CVE users should reference CVE-2020-25905 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2018-12125	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2017-1061	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1060	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1059	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1058	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1043	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1044	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1045	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-1046	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1047	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1048	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2018-12165	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2017-1050	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1051	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1052	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1053	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1054	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1055	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2017-1056	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-1057	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2017. Notes: none.	N/A	More Details
CVE-2018-12128	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-12129	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-12132	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18185	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18183	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18182	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18181	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18180	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18179	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18178	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18177	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-18176	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18175	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18174	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18173	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18172	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18171	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18170	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18169	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18184	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18186	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-12133	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18187	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-12134	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-12135	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-12136	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-12138	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-12139	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-12140	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-12141	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-12142	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-12143	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-12144	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-12145	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-12146	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-12156	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-12157	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-18188	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details
CVE-2018-12137	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues. Notes: none.	N/A	More Details