SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 25 January 2023

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-45444	Sewio's Real-Time Location System (RTLS) Studio version 2.0.0 up to and including version 2.6.2 contains hard-coded passwords for select users in the application's database. This could allow a remote attacker to login to the database with unrestricted access.	10.0	More Details
CVE-2022-46732	Even if the authentication fails for local service authentication, the requested command could still execute regardless of authentication status.	9.8	More Details
CVE-2023-0052	SAUTER Controls Nova 200–220 Series with firmware version 3.3-006 and prior and BACnetstac version 4.2.1 and prior allows the execution of commands without credentials. As Telnet and file transfer protocol (FTP) are the only protocols available for device management, an unauthorized user could access the system and modify the device configuration, which could result in the unauthorized user executing unrestricted malicious commands.	9.8	More Details
CVE-2020-21152	SQL Injection vulnerability in inxedu 2.0.6 allows attackers to execute arbitrary commands via the functionIds parameter to /saverolefunction.	9.8	More Details
CVE-2020-22653	In Ruckus R310 10.5.1.0.199, Ruckus R500 10.5.1.0.199, Ruckus R600 10.5.1.0.199, Ruckus T300 10.5.1.0.199, Ruckus T301n 10.5.1.0.199, Ruckus T301s 10.5.1.0.199, SmartCell Gateway 200 (SCG200) before 3.6.2.0.795, SmartZone 100 (SZ-100) before 3.6.2.0.795, SmartZone 300 (SZ300) before 3.6.2.0.795, Virtual SmartZone (vSZ) before 3.6.2.0.795, ZoneDirector 1100 9.10.2.0.130, ZoneDirector 1200 10.2.1.0.218, ZoneDirector 3000 10.2.1.0.218, ZoneDirector 5000 10.0.1.0.151, a vulnerability allows attackers to exploit the official image signature to force injection unauthorized image signature.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-22654	In Ruckus R310 10.5.1.0.199, Ruckus R500 10.5.1.0.199, Ruckus R600 10.5.1.0.199, Ruckus T300 10.5.1.0.199, Ruckus T301n 10.5.1.0.199, Ruckus T301s 10.5.1.0.199, SmartCell Gateway 200 (SCG200) before 3.6.2.0.795, SmartZone 100 (SZ-100) before 3.6.2.0.795, SmartZone 300 (SZ300) before 3.6.2.0.795, Virtual SmartZone (vSZ) before 3.6.2.0.795, ZoneDirector 1100 9.10.2.0.130, ZoneDirector 1200 10.2.1.0.218, ZoneDirector 3000 10.2.1.0.218, ZoneDirector 5000 10.0.1.0.151, a vulnerability allows attackers to bypass firmware image bad md5 checksum failed error.	9.8	More Details
CVE-2020-22658	In Ruckus R310 10.5.1.0.199, Ruckus R500 10.5.1.0.199, Ruckus R600 10.5.1.0.199, Ruckus T300 10.5.1.0.199, Ruckus T301n 10.5.1.0.199, Ruckus T301s 10.5.1.0.199, SmartCell Gateway 200 (SCG200) before 3.6.2.0.795, SmartZone 100 (SZ-100) before 3.6.2.0.795, SmartZone 300 (SZ300) before 3.6.2.0.795, Virtual SmartZone (vSZ) before 3.6.2.0.795, ZoneDirector 1100 9.10.2.0.130, ZoneDirector 1200 10.2.1.0.218, ZoneDirector 3000 10.2.1.0.218, ZoneDirector 5000 10.0.1.0.151, a vulnerability allows attackers to switch completely to unauthorized image to be Boot as primary verified image.	9.8	More Details
CVE-2020-23256	An issue was discovered in Electerm 1.3.22, allows attackers to execute arbitrary code via unverified request to electerms service.	9.8	More Details
CVE-2020-29297	Multiple SQL Injection vulnerabilities in tourist5 Online-food-ordering-system 1.0.	9.8	More Details
CVE-2022-48120	SQL Injection vulnerability in kishan0725 Hospital Management System thru commit 4770d740f2512693ef8fd9aa10a8d17f79fad9bd (on March 13, 2021), allows attackers to execute arbitrary commands via the contact and doctor parameters to /search.php.	9.8	More Details
CVE-2022-48152	SQL Injection vulnerability in RemoteClinic 2.0 allows attackers to execute arbitrary commands and gain sensitive information via the id parameter to /medicines/profile.php.	9.8	More Details
CVE-2023-23607	erohtar/Dasherr is a dashboard for self-hosted services. In affected versions unrestricted file upload allows any unauthenticated user to execute arbitrary code on the server. The file /www/include/filesave.php allows for any file to uploaded to anywhere. If an attacker uploads a php file they can execute code on the server. This issue has been addressed in version 1.05.00. Users are advised to upgrade. There are no known workarounds for this issue.	9.8	More Details
CVE-2023-24028	In MISP 2.4.167, app/Controller/Component/ACLComponent.php has incorrect access control for the decaying import function.	9.8	More Details
CVE-2023-21890	Vulnerability in the Oracle Communications Converged Application Server product of Oracle Communications (component: Core). Supported versions that are affected are 7.1.0 and 8.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via UDP to compromise Oracle Communications Converged Application Server. Successful attacks of this vulnerability can result in takeover of Oracle Communications Converged Application Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2023-22884	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in Apache Software Foundation Apache Airflow, Apache Software Foundation Apache Airflow MySQL Provider.This issue affects Apache Airflow: before 2.5.1; Apache Airflow MySQL Provider: before 4.0.0.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0435	Excessive Attack Surface in GitHub repository pyload/pyload prior to 0.5.0b3.dev41.	9.8	More Details
CVE-2021-43445	ONLYOFFICE all versions as of 2021-11-08 is affected by Incorrect Access Control. An attacker can authenticate with the web socket service of the ONLYOFFICE document editor which is protected by JWT auth by using a default JWT signing key.	9.8	More Details
CVE-2022-0316	The WeStand WordPress theme before 2.1, footysquare WordPress theme, aidreform WordPress theme, statfort WordPress theme, club-theme WordPress theme, kingclub-theme WordPress theme, spikes WordPress theme, spikes-black WordPress theme, soundblast WordPress theme, bolster WordPress theme from ChimpStudio and PixFill does not have any authorisation and upload validation in the lang_upload.php file, allowing any unauthenticated attacker to upload arbitrary files to the web server.	9.8	More Details
CVE-2022-4305	The Login as User or Customer WordPress plugin before 3.3 lacks authorization checks to ensure that users are allowed to log in as another one, which could allow unauthenticated attackers to obtain a valid admin session.	9.8	More Details
CVE-2022-4383	The CBX Petition for WordPress plugin through 1.0.3 does not properly sanitize and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection.	9.8	More Details
CVE-2022-4693	The User Verification WordPress plugin before 1.0.94 was affected by an Auth Bypass security vulnerability. To bypass authentication, we only need to know the user’s username. Depending on whose username we know, which can be easily queried because it is usually public data, we may even be given an administrative role on the website.	9.8	More Details
CVE-2023-23560	In certain Lexmark products through 2023-01-12, SSRF can occur because of a lack of input validation.	9.8	More Details
CVE-2023-23489	The Easy Digital Downloads WordPress Plugin, versions 3.1.0.2 & 3.1.0.3, is affected by an unauthenticated SQL injection vulnerability in the 's' parameter of its 'edd_download_search' action.	9.8	More Details
CVE-2023-23488	The Paid Memberships Pro WordPress Plugin, version < 2.9.8, is affected by an unauthenticated SQL injection vulnerability in the 'code' parameter of the '/pmpro/v1/order' REST route.	9.8	More Details
CVE-2022-46887	Multiple SQL injection vulnerabilities in NexusPHP before 1.7.33 allow remote attackers to execute arbitrary SQL commands via the conuser[] parameter in takeconfirm.php; the delcheater parameter in cheaterbox.php; or the usernw parameter in nowarn.php.	9.8	More Details
CVE-2022-46476	D-Link DIR-859 A1 1.05 was discovered to contain a command injection vulnerability via the service= variable in the soapcgi_main function.	9.8	More Details
CVE-2022-41417	BlogEngine.NET v3.3.8.0 allows an attacker to create any folder with "files" prefix under ~/App_Data/.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47966	Multiple Zoho ManageEngine on-premise products, such as ServiceDesk Plus through 14003, allow remote code execution due to use of Apache Santuario xmlsec (aka XML Security for Java) 1.4.1, because the xmlsec XSLT features, by design in that version, make the application responsible for certain security protections, and the ManageEngine applications did not provide those protections. This affects Access Manager Plus before 4308, Active Directory 360 before 4310, ADAudit Plus before 7081, ADManager Plus before 7162, ADSelfService Plus before 6211, Analytics Plus before 5150, Application Control Plus before 10.1.2220.18, Asset Explorer before 6983, Browser Security Plus before 11.1.2238.6, Device Control Plus before 10.1.2220.18, Endpoint Central before 10.1.2228.11, Endpoint Central MSP before 10.1.2228.11, Endpoint DLP before 10.1.2137.6, Key Manager Plus before 6401, OS Deployer before 1.1.2243.1, PAM 360 before 5713, Password Manager Pro before 12124, Patch Manager Plus before 10.1.2220.18, Remote Access Plus before 10.1.2228.11, Remote Monitoring and Management (RMM) before 10.1.41. ServiceDesk Plus before 14004, ServiceDesk Plus MSP before 13001, SupportCenter Plus before 11026, and Vulnerability Manager Plus before 10.1.2220.18. Exploitation is only possible if SAML SSO has ever been configured for a product (for some products, exploitation requires that SAML SSO is currently active).	9.8	More Details
CVE-2020-35326	SQL Injection vulnerability in file /inxedu/demo_inxedu_open/src/main/resources/mybatis/inxedu/website/WebsiteImagesMapper.xml in inxedu 2.0.6 via the id value.	9.8	More Details
CVE-2022-47105	Jeecg-boot v3.4.4 was discovered to contain a SQL injection vulnerability via the component /sys/dict/queryTableData.	9.8	More Details
CVE-2022-47740	Seltmann GmbH Content Management System 6 is vulnerable to SQL Injection via /index.php.	9.8	More Details
CVE-2022-48126	TOTOlink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability via the username parameter in the setting/setOpenVpnCertGenerationCfg function.	9.8	More Details
CVE-2023-22741	Sofia-SIP is an open-source SIP User-Agent library, compliant with the IETF RFC3261 specification. In affected versions Sofia-SIP **lacks both message length and attributes length checks** when it handles STUN packets, leading to controllable heap-over-flow. For example, in stun_parse_attribute(), after we get the attribute's type and length value, the length will be used directly to copy from the heap, regardless of the message's left size. Since network users control the overflowed length, and the data is written to heap chunks later, attackers may achieve remote code execution by heap grooming or other exploitation methods. The bug was introduced 16 years ago in sofia-sip 1.12.4 (plus some patches through 12/21/2006) to in tree libs with git-svn-id: http://svn.freeswitch.org/svn/freeswitch/trunk@3774 d0543943-73ff-0310-b7d9-9358b9ac24b2. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.8	More Details
CVE-2023-23331	Amano Xoffice parking solutions 7.1.3879 is vulnerable to SQL Injection.	9.8	More Details
CVE-2022-48121	TOTOlink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability via the rsabits parameter in the setting/delStaticDhcpRules function.	9.8	More Details
CVE-2022-48122	TOTOlink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability via the dayvalid parameter in the setting/delStaticDhcpRules function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48123	TOTOlink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability via the servername parameter in the setting/delStaticDhcpRules function.	9.8	More Details
CVE-2022-48124	TOTOlink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability via the FileName parameter in the setting/setOpenVpnCertGenerationCfg function.	9.8	More Details
CVE-2022-48125	TOTOlink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability via the password parameter in the setting/setOpenVpnCertGenerationCfg function.	9.8	More Details
CVE-2023-0397	A malicious / defect bluetooth controller can cause a Denial of Service due to unchecked input in le_read_buffer_size_complete.	9.6	More Details
CVE-2020-22657	In Ruckus R310 10.5.1.0.199, Ruckus R500 10.5.1.0.199, Ruckus R600 10.5.1.0.199, Ruckus T300 10.5.1.0.199, Ruckus T301n 10.5.1.0.199, Ruckus T301s 10.5.1.0.199, SmartCell Gateway 200 (SCG200) before 3.6.2.0.795, SmartZone 100 (SZ-100) before 3.6.2.0.795, SmartZone 300 (SZ300) before 3.6.2.0.795, Virtual SmartZone (vSZ) before 3.6.2.0.795, ZoneDirector 1100 9.10.2.0.130, ZoneDirector 1200 10.2.1.0.218, ZoneDirector 3000 10.2.1.0.218, ZoneDirector 5000 10.0.1.0.151, a vulnerability allows attackers to perform WEB GUI login authentication bypass.	9.1	More Details
CVE-2022-47911	Sewio's Real-Time Location System (RTLS) Studio version 2.0.0 up to and including version 2.6.2 does not properly validate the input module name to the backup services of the software. This could allow a remote attacker to access sensitive functions of the application and execute arbitrary system commands.	9.1	More Details
CVE-2022-43483	Sewio's Real-Time Location System (RTLS) Studio version 2.0.0 up to and including version 2.6.2 does not properly validate the input module name to the monitor services of the software. This could allow a remote attacker to access sensitive functions of the application and execute arbitrary system commands.	9.1	More Details
CVE-2023-22964	Zoho ManageEngine ServiceDesk Plus MSP before 10611, and 13x before 13004, is vulnerable to authentication bypass when LDAP authentication is enabled.	9.1	More Details
CVE-2023-20025	A vulnerability in the web-based management interface of Cisco Small Business RV042 Series Routers could allow an unauthenticated, remote attacker to bypass authentication on the affected device. This vulnerability is due to incorrect user input validation of incoming HTTP packets. An attacker could exploit this vulnerability by sending crafted requests to the web-based management interface. A successful exploit could allow the attacker to gain root privileges on the affected device.	9.0	More Details
CVE-2022-41989	Sewio's Real-Time Location System (RTLS) Studio version 2.0.0 up to and including version 2.6.2 does not validate the length of RTLS report payloads during communication. This allows an attacker to send an exceedingly long payload, resulting in an out-of-bounds write to cause a denial-of-service condition or code execution.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference

CVE Number	Description	Base Score	Reference
CVE-2023-24097	TrendNet Wireless AC Easy-Upgrader TEW-820AP v1.0R, firmware version 1.01.B01 was discovered to contain a stack overflow via the submit-url parameter at /formPasswordAuth. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2022-45927	An issue was discovered in OpenText Content Suite Platform 22.1 (16.2.19.1803). The Java application server can be used to bypass the authentication of the QDS endpoints of the Content Server. These endpoints can be used to create objects and execute arbitrary code.	8.8	More Details
CVE-2022-4017	The Booster for WooCommerce WordPress plugin before 6.0.1, Booster Plus for WooCommerce WordPress plugin before 6.0.1, Booster Elite for WooCommerce WordPress plugin before 6.0.1 have either flawed CSRF checks or are missing them completely in numerous places, allowing attackers to make logged in users perform unwanted actions via CSRF attacks	8.8	More Details
CVE-2023-24095	TrendNet Wireless AC Easy-Upgrader TEW-820AP v1.0R, firmware version 1.01.B01 was discovered to contain a stack overflow via the submit-url parameter at /formSystemCheck. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2023-23490	The Survey Maker WordPress Plugin, version < 3.1.2, is affected by an authenticated SQL injection vulnerability in the 'surveys_ids' parameter of its 'ays_surveys_export_json' action.	8.8	More Details
CVE-2023-21846	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Security). Supported versions that are affected are 5.9.0.0.0, 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in takeover of Oracle BI Publisher. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2022-45748	An issue was discovered with assimp 5.1.4, a use after free occurred in function ColladaParser::ExtractDataObjectFromChannel in file /code/AssetLib/Collada/ColladaParser.cpp.	8.8	More Details
CVE-2023-21848	Vulnerability in the Oracle Communications Convergence product of Oracle Communications Applications (component: Admin Configuration). The supported version that is affected is 3.0.3.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Communications Convergence. Successful attacks of this vulnerability can result in takeover of Oracle Communications Convergence. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2023-20038	A vulnerability in the monitoring application of Cisco Industrial Network Director could allow an authenticated, local attacker to access a static secret key used to store both local data and credentials for accessing remote systems. This vulnerability is due to a static key value stored in the application used to encrypt application data and remote credentials. An attacker could exploit this vulnerability by gaining local access to the server Cisco Industrial Network Director is installed on. A successful exploit could allow the attacker to decrypt data allowing the attacker to access remote systems monitored by Cisco Industrial Network Director.	8.8	More Details
CVE-2020-36655	Yii Yii2 Gii before 2.2.2 allows remote attackers to execute arbitrary code via the Generator.php messageCategory field. The attacker can embed arbitrary PHP code into the model file.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0164	OrangeScrum version 2.0.11 allows an authenticated external attacker to execute arbitrary commands on the server. This is possible because the application injects an attacker-controlled parameter into a system function.	8.8	More Details
CVE-2022-45923	An issue was discovered in OpenText Content Suite Platform 22.1 (16.2.19.1803). The Common Gateway Interface (CGI) program cs.exe allows an attacker to increase/decrease an arbitrary memory address by 1 and trigger a call to a method of a vftable with a vftable pointer value chosen by the attacker.	8.8	More Details
CVE-2023-23492	The Login with Phone Number WordPress Plugin, version < 1.4.2, is affected by an authenticated SQL injection vulnerability in the 'ID' parameter of its 'lwp_forgot_password' action.	8.8	More Details
CVE-2023-0242	Rapid7 Velociraptor allows users to be created with different privileges on the server. Administrators are generally allowed to run any command on the server including writing arbitrary files. However, lower privilege users are generally forbidden from writing or modifying files on the server. The VQL copy() function applies permission checks for reading files but does not check for permission to write files. This allows a low privilege user (usually, users with the Velociraptor "investigator" role) to overwrite files on the server, including Velociraptor configuration files. To exploit this vulnerability, the attacker must already have a Velociraptor user account at a low privilege level (at least "analyst") and be able to log into the GUI and create a notebook where they can run the VQL query invoking the copy() VQL function. Typically, most users deploy Velociraptor with limited access to a trusted group (most users will be administrators within the GUI). This vulnerability is associated with program files https://github.Com/Velocidex/velociraptor/blob/master/vql/filesystem/copy.go https://github.Com/Velocidex/velociraptor/blob/master/vql/filesystem/copy.go and program routines copy(). This issue affects Velociraptor versions before 0.6.7-5. Version 0.6.7-5, released January 16, 2023, fixes the issue.	8.8	More Details
CVE-2022-45928	A remote OScript execution issue was discovered in OpenText Content Suite Platform 22.1 (16.2.19.1803). Multiple endpoints allow the user to pass the parameter htmlFile, which is included in the HTML output rendering pipeline of a request. Because the Content Server evaluates and executes Oscript code in HTML files, it is possible for an attacker to execute Oscript code. The Oscript scripting language allows the attacker (for example) to manipulate files on the filesystem, create new network connections, or execute OS commands.	8.8	More Details
CVE-2022-45926	An issue was discovered in OpenText Content Suite Platform 22.1 (16.2.19.1803). The endpoint notify.localizeEmailTemplate allows a low-privilege user to evaluate webreports.	8.8	More Details
CVE-2022-37719	A Cross-Site Request Forgery (CSRF) in the management portal of JetNexus/EdgeNexus ADC 4.2.8 allows attackers to escalate privileges and execute arbitrary code via unspecified vectors.	8.8	More Details
CVE-2022-37718	The management portal component of JetNexus/EdgeNexus ADC 4.2.8 was discovered to contain a command injection vulnerability. This vulnerability allows authenticated attackers to execute arbitrary commands through a specially crafted payload. This vulnerability can also be exploited from an unauthenticated context via unspecified vectors	8.8	More Details
CVE-2022-45922	An issue was discovered in OpenText Content Suite Platform 22.1 (16.2.19.1803). The request handler for ll.KeepAliveSession sets a valid AdminPwd cookie even when the Web Admin password was not entered. This allows access to endpoints, which require a valid AdminPwd cookie, without knowing the password.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24099	TrendNet Wireless AC Easy-Upgrader TEW-820AP v1.0R, firmware version 1.01.B01 was discovered to contain a stack overflow via the username parameter at /formWizardPassword. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2023-24098	TrendNet Wireless AC Easy-Upgrader TEW-820AP v1.0R, firmware version 1.01.B01 was discovered to contain a stack overflow via the submit-url parameter at /formSysLog. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2023-0101	A privilege escalation vulnerability was identified in Nessus versions 8.10.1 through 8.15.8 and 10.0.0 through 10.4.1. An authenticated attacker could potentially execute a specially crafted file to obtain root or NT AUTHORITY / SYSTEM privileges on the Nessus host.	8.8	More Details
CVE-2022-47065	TrendNet Wireless AC Easy-Upgrader TEW-820AP v1.0R, firmware version 1.01.B01 was discovered to contain a stack overflow via the submit-url parameter at /formNewSchedule. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2022-4230	The WP Statistics WordPress plugin before 13.2.9 does not escape a parameter, which could allow authenticated users to perform SQL Injection attacks. By default, the affected feature is available to users with the manage_options capability (admin+), however the plugin has a settings to allow low privilege users to access it as well.	8.8	More Details
CVE-2023-24096	TrendNet Wireless AC Easy-Upgrader TEW-820AP v1.0R, firmware version 1.01.B01 was discovered to contain a stack overflow via the newpass parameter at /formPasswordSetup. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2022-47766	PopojiCMS v2.0.1 backend plugin function has a file upload vulnerability.	8.8	More Details
CVE-2021-29368	Session fixation vulnerability in CuppaCMS thru commit 4c9b742b23b924cf4c1f943f48b278e06a17e297 on November 12, 2019 allows attackers to gain access to arbitrary user sessions.	8.8	More Details
CVE-2023-23314	An arbitrary file upload vulnerability in the /api/upload component of zdir v3.2.0 allows attackers to execute arbitrary code via a crafted .ssh file.	8.8	More Details
CVE-2021-26642	When uploading an image file to a bulletin board developed with XpressEngine, a vulnerability in which an arbitrary file can be uploaded due to insufficient verification of the file. A remote attacker can use this vulnerability to execute arbitrary code on the server where the bulletin board is running.	8.8	More Details
CVE-2021-26644	SQL-Injection vulnerability caused by the lack of verification of input values for the table name of DB used by the Mangboard bulletin board. A remote attacker can use this vulnerability to execute arbitrary code on the server where the bulletin board is running.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3918	A program using FoundationNetworking in swift-corelibs-foundation is potentially vulnerable to CRLF ( ) injection in URLRequest headers. In this vulnerability, a client can insert one or several CRLF sequences into a URLRequest header value. When that request is sent via URLSession to an HTTP server, the server may interpret the content after the CRLF as extra headers, or even a second request. For example, consider a URLRequest to http://example.com/ with the GET method. Suppose we set the URLRequest header "Foo" to the value "Bar Extra-Header: Added GET /other HTTP/1.1". When this request is sent, it will appear to the server as two requests: GET / HTTP/1.1 Foo: Bar Extra-Header: Added GET /other HTTP/1.1 In this manner, the client is able to inject extra headers and craft an entirely new request to a separate path, despite only making one API call in URLSession. If a developer has total control over the request and its headers, this vulnerability may not pose a threat. However, this vulnerability escalates if un-sanitized user input is placed in header values. If so, a malicious user could inject new headers or requests to an intermediary or backend server. Developers should be especially careful to sanitize user input in this case, or upgrade their version of swift-corelibs-foundation to include the patch below.	8.8	More Details
CVE-2022-47745	ZenTao 16.4 to 18.0.beta1 is vulnerable to SQL injection. After logging in with any user, you can complete SQL injection by constructing a special request and sending it to function importNotice.	8.8	More Details
CVE-2023-21832	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Security). Supported versions that are affected are 5.9.0.0.0, 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in takeover of Oracle BI Publisher. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2022-34456	Dell EMC Metro node, Version(s) prior to 7.1, contain a Code Injection Vulnerability. An authenticated nonprivileged attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application.	8.8	More Details
CVE-2023-23596	jc21 NGINX Proxy Manager through 2.9.19 allows OS command injection. When creating an access list, the backend builds an htpasswd file with crafted username and/or password input that is concatenated without any validation, and is directly passed to the exec command, potentially allowing an authenticated attacker to execute arbitrary commands on the system. NOTE: this is not part of any NGINX software shipped by F5.	8.8	More Details
CVE-2022-23005	Western Digital has identified a weakness in the UFS standard that could result in a security vulnerability. This vulnerability may exist in some systems where the Host boot ROM code implements the UFS Boot feature to boot from UFS compliant storage devices. The UFS Boot feature, as specified in the UFS standard, is provided by UFS devices to support platforms that need to download the system boot loader from external non-volatile storage locations. Several scenarios have been identified in which adversaries may disable the boot capability, or revert to an old boot loader code, if the host boot ROM code is improperly implemented. UFS Host Boot ROM implementers may be impacted by this vulnerability. UFS devices are only impacted when connected to a vulnerable UFS Host and are not independently impacted by this vulnerability. When present, the vulnerability is in the UFS Host implementation and is not a vulnerability in Western Digital UFS Devices. Western Digital has provided details of the vulnerability to the JEDEC standards body, multiple vendors of host processors, and software solutions providers.	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20020	A vulnerability in the Device Management Servlet application of Cisco BroadWorks Application Delivery Platform and Cisco BroadWorks Xtended Services Platform could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper input validation when parsing HTTP requests. An attacker could exploit this vulnerability by sending a sustained stream of crafted requests to an affected device. A successful exploit could allow the attacker to cause all subsequent requests to be dropped, resulting in a DoS condition.	8.6	More Details
CVE-2023-20018	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication.	8.6	More Details
CVE-2022-34462	Dell EMC SCG Policy Manager, versions from 5.10 to 5.12, contain(s) a Hard-coded Password Vulnerability. An attacker, with the knowledge of the hard-coded credentials, could potentially exploit this vulnerability to login to the system to gain admin privileges.	8.4	More Details
CVE-2023-21775	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	8.3	More Details
CVE-2023-21795	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	8.3	More Details
CVE-2023-21796	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	8.3	More Details
CVE-2022-45924	An issue was discovered in OpenText Content Suite Platform 22.1 (16.2.19.1803). The endpoint itemtemplate.createtemplate2 allows a low-privilege user to delete arbitrary files on the server's local filesystem.	8.1	More Details
CVE-2022-47395	Sewio’s Real-Time Location System (RTLS) Studio version 2.0.0 up to and including version 2.6.2 is vulnerable to cross-site request forgery in its monitor services. An attacker could take advantage of this vulnerability to execute arbitrary maintenance operations and cause a denial-of-service condition.	8.1	More Details
CVE-2021-43449	ONLYOFFICE all versions as of 2021-11-08 is vulnerable to Server-Side Request Forgery (SSRF). The document editor service can be abused to read and serve arbitrary URLs as a document.	8.1	More Details
CVE-2023-21862	Vulnerability in the Oracle Web Services Manager product of Oracle Fusion Middleware (component: XML Security component). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Web Services Manager. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Web Services Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Web Services Manager accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45127	Sewio's Real-Time Location System (RTLS) Studio version 2.0.0 up to and including version 2.6.2 is vulnerable to cross-site request forgery in its backup services. An attacker could take advantage of this vulnerability to execute arbitrary backup operations and cause a denial-of-service condition.	8.1	More Details
CVE-2023-20010	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability exists because the web-based management interface inadequately validates user input. An attacker could exploit this vulnerability by authenticating to the application as a low-privileged user and sending crafted SQL queries to an affected system. A successful exploit could allow the attacker to read or modify any data on the underlying database or elevate their privileges.	8.1	More Details
CVE-2021-37500	Directory traversal vulnerability in Reprise License Manager (RLM) web interface before 14.2BL4 in the diagnostics function that allows RLM users with sufficient privileges to overwrite any file the on the server.	8.1	More Details
CVE-2023-21886	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	8.1	More Details
CVE-2023-23691	Dell EMC PV ME5, versions ME5.1.0.0.0 and ME5.1.0.1.0, contains a Client-side desync Vulnerability. An unauthenticated attacker could potentially exploit this vulnerability to force a victim's browser to desynchronize its connection with the website, typically leading to XSS and DoS.	8.1	More Details
CVE-2023-21828	Vulnerability in the Oracle Hospitality Reporting and Analytics product of Oracle Food and Beverage Applications (component: Reporting). The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Hospitality Reporting and Analytics. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized access to critical data or complete access to all Oracle Hospitality Reporting and Analytics accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2023-22726	act is a project which allows for local running of github actions. The artifact server that stores artifacts from Github Action runs does not sanitize path inputs. This allows an attacker to download and overwrite arbitrary files on the host from a Github Action. This issue may lead to privilege escalation. The /upload endpoint is vulnerable to path traversal as filepath is user controlled, and ultimately flows into os.Mkdir and os.Open. The /artifact endpoint is vulnerable to path traversal as the path is variable is user controlled, and the specified file is ultimately returned by the server. This has been addressed in version 0.2.40. Users are advised to upgrade. Users unable to upgrade may, during implementation of Open and OpenAtEnd for FS, ensure to use ValidPath() to check against path traversal or clean the user-provided paths manually.	8.0	More Details
CVE-2022-34442	Dell EMC SCG Policy Manager, versions from 5.10 to 5.12, contain(s) a contain a Hard-coded Cryptographic Key vulnerability. An attacker with the knowledge of the hard-coded sensitive information, could potentially exploit this vulnerability to login to the system to gain LDAP user privileges.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37774	An issue was discovered in function httpProcDataSrv in TL-WDR7660 2.0.30 that allows attackers to execute arbitrary code.	8.0	More Details
CVE-2023-23145	GPAC version 2.2-rev0-gab012bbfb-master was discovered to contain a memory leak in lsr_read_rare_full function.	7.8	More Details
CVE-2022-45639	OS Command injection vulnerability in sleuthkit fls tool 4.11.1 allows attackers to execute arbitrary commands via a crafted value to the m parameter. NOTE: third parties have disputed this because there is no analysis showing that the backtick command executes outside the context of the user account that entered the command line.	7.8	More Details
CVE-2022-25631	Symantec Endpoint Protection, prior to 14.3 RU6 (14.3.9210.6000), may be susceptible to a Elevation of Privilege vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated	7.8	More Details
CVE-2023-0433	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.1225.	7.8	More Details
CVE-2022-47024	A null pointer dereference issue was discovered in function gui_x11_create_blank_mouse in gui_x11.c in vim 8.1.2269 thru 9.0.0339 allows attackers to cause denial of service or other unspecified impacts.	7.8	More Details
CVE-2021-33641	When processing files, malloc stores the data of the current line. When processing comments, malloc incorrectly accesses the released memory (use after free).	7.8	More Details
CVE-2023-21579	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2020-25502	Cybereason EDR version 19.1.282 and above, 19.2.182 and above, 20.1.343 and above, and 20.2.X and above has a DLL hijacking vulnerability, which could allow a local attacker to execute code with elevated privileges.	7.8	More Details
CVE-2023-21604	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-0358	Use After Free in GitHub repository gpac/gpac prior to 2.3.0-DEV.	7.8	More Details
CVE-2023-24068	Signal Desktop before 6.2.0 on Windows, Linux, and macOS allows an attacker to modify conversation attachments within the attachments.noindex directory. Client mechanisms fail to validate modifications of existing cached files, resulting in an attacker's ability to insert malicious code into pre-existing attachments or replace them completely. A threat actor can forward the existing attachment in the corresponding conversation to external groups, and the name and size of the file will not change, allowing the malware to masquerade as another file. NOTE: the vendor disputes the relevance of this finding because the product is not intended to protect against adversaries with this degree of local access.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21605	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-21606	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-21607	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-21608	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-21609	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-21610	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-21611	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-21612	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-24039	A stack-based buffer overflow in ParseColors in libXm in Common Desktop Environment 1.6 can be exploited by local low-privileged users via the dtprintinfo setuid binary to escalate their privileges to root on Solaris 10 systems. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	7.8	More Details
CVE-2022-3085	Fuji Electric Tellus Lite V-Simulator versions 4.0.12.0 and prior are vulnerable to a stack-based buffer overflow which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2023-23143	Buffer overflow vulnerability in function avc_parse_slice in file media_tools/av_parsers.c. GPAC version 2.3-DEV-rev1-g4669ba229-master.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47021	A null pointer dereference issue was discovered in functions op_get_data and op_open1 in opusfile.c in xiph opusfile 0.9 thru 0.12 allows attackers to cause denial of service or other unspecified impacts.	7.8	More Details
CVE-2023-22809	In Sudo before 1.9.12p2, the sudoedit (aka -e) feature mishandles extra arguments passed in the user-provided environment variables (SUDO_EDITOR, VISUAL, and EDITOR), allowing a local attacker to append arbitrary entries to the list of files to process. This can lead to privilege escalation. Affected versions are 1.8.0 through 1.9.12.p1. The problem exists because a user-specified editor may contain a "--" argument that defeats a protection mechanism, e.g., an EDITOR='vim -- /path/to/extra/file' value.	7.8	More Details
CVE-2023-21826	Vulnerability in the Oracle Hospitality Reporting and Analytics product of Oracle Food and Beverage Applications (component: Reporting). The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Hospitality Reporting and Analytics. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Reporting and Analytics accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hospitality Reporting and Analytics. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:H).	7.6	More Details
CVE-2022-45925	An issue was discovered in OpenText Content Suite Platform 22.1 (16.2.19.1803). The action xmlexport accepts the parameter requestContext. If this parameter is present, the response includes most of the HTTP headers sent to the server and some of the CGI variables like remote_adde and server_name, which is an information disclosure.	7.5	More Details
CVE-2023-24025	CRYSTALS-DILITHIUM (in Post-Quantum Cryptography Selected Algorithms 2022) in PQClean d03da30 may allow universal forgeries of digital signatures via a template side-channel attack because of intermediate data leakage of one vector.	7.5	More Details
CVE-2023-0126	Pre-authentication path traversal vulnerability in SMA1000 firmware version 12.4.2, which allows an unauthenticated attacker to access arbitrary files and directories stored outside the web root directory.	7.5	More Details
CVE-2021-33959	Plex media server 1.21 and before is vulnerable to ddos reflection attack via plex service.	7.5	More Details
CVE-2022-47732	In Yeastar N412 and N824 Configuration Panel 42.x and 45.x, an unauthenticated attacker can create backup file and download it, revealing admin hash, allowing, once cracked, to login inside the Configuration Panel, otherwise, replacing the hash in the archive and restoring it on the device which will change admin password granting access to the device.	7.5	More Details
CVE-2021-36630	DDOS reflection amplification vulnerability in eAut module of Ruckus Wireless SmartZone controller that allows remote attackers to perform DOS attacks via crafted request.	7.5	More Details
CVE-2021-43447	ONLYOFFICE all versions as of 2021-11-08 is affected by Incorrect Access Control. An authentication bypass in the document editor allows attackers to edit documents without authentication.	7.5	More Details
CVE-2023-22331	Use of default credentials vulnerability in CONPROSYS HMI System (CHS) Ver.3.4.5 and earlier allows a remote unauthenticated attacker to alter user credentials information.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0434	Improper Input Validation in GitHub repository pyload/pyload prior to 0.5.0b3.dev40.	7.5	More Details
CVE-2023-22617	A remote attacker might be able to cause infinite recursion in PowerDNS Recursor 4.8.0 via a DNS query that retrieves DS records for a misconfigured domain, because QName minimization is used in QM fallback mode. This is fixed in 4.8.1.	7.5	More Details
CVE-2021-24881	The Passster WordPress plugin before 3.5.5.9 does not properly check for password, as well as that the post to be viewed is public, allowing unauthenticated users to bypass the protection offered by the plugin, and access arbitrary posts (such as private) content, by sending a specifically crafted request.	7.5	More Details
CVE-2022-46505	An issue in MatrixSSL 4.5.1-open and earlier leads to failure to securely check the SessionID field, resulting in the misuse of an all-zero MasterSecret that can decrypt secret data.	7.5	More Details
CVE-2021-43444	ONLYOFFICE all versions as of 2021-11-08 is affected by Incorrect Access Control. Signed document download URLs can be forged due to a weak default URL signing key.	7.5	More Details
CVE-2023-0040	Versions of Async HTTP Client prior to 1.13.2 are vulnerable to a form of targeted request manipulation called CRLF injection. This vulnerability was the result of insufficient validation of HTTP header field values before sending them to the network. Users are vulnerable if they pass untrusted data into HTTP header field values without prior sanitisation. Common use-cases here might be to place usernames from a database into HTTP header fields. This vulnerability allows attackers to inject new HTTP header fields, or entirely new requests, into the data stream. This can cause requests to be understood very differently by the remote server than was intended. In general, this is unlikely to result in data disclosure, but it can result in a number of logical errors and other misbehaviours.	7.5	More Details
CVE-2023-24042	A race condition in LightFTP through 2.2 allows an attacker to achieve path traversal via a malformed FTP request. A handler thread can use an overwritten context->FileName.	7.5	More Details
CVE-2022-4303	The WP Limit Login Attempts WordPress plugin through 2.6.4 prioritizes getting a visitor's IP from certain HTTP headers over PHP's REMOTE_ADDR, which makes it possible to bypass IP-based restrictions on login forms.	7.5	More Details
CVE-2023-24038	The HTML-StripScripts module through 1.06 for Perl allows _hss_attval_style ReDoS because of catastrophic backtracking for HTML content with certain style attributes.	7.5	More Details
CVE-2022-47747	kraken <= 0.1.4 has an arbitrary file read vulnerability via the component testfs.	7.5	More Details
CVE-2023-22339	Improper access control vulnerability in CONPROSYS HMI System (CHS) Ver.3.4.5 and earlier allows a remote unauthenticated attacker to bypass access restriction and obtain the server certificate including the private key of the product.	7.5	More Details
CVE-2022-38725	An integer overflow in the RFC3164 parser in One Identity syslog-ng 3.0 through 3.37 allows remote attackers to cause a Denial of Service via crafted syslog input that is mishandled by the tcp or network function. syslog-ng Premium Edition 7.0.30 and syslog-ng Store Box 6.10.0 are also affected.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46331	An unauthorized user could possibly delete any file on the system.	7.5	More Details
CVE-2022-46660	An unauthorized user could alter or write files with full control over the path and content of the file.	7.5	More Details
CVE-2022-46639	A vulnerability in the descarga_etiqueta.php component of Correos Prestashop 1.7.x allows attackers to execute a directory traversal.	7.5	More Details
CVE-2022-4746	The FluentAuth WordPress plugin before 1.0.2 prioritizes getting a visitor's IP address from certain HTTP headers over PHP's REMOTE_ADDR, which makes it possible to bypass the IP-based blocks set by the plugin.	7.5	More Details
CVE-2023-21837	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2023-21838	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2023-21839	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2022-47012	Use of uninitialized variable in function gen_eth_recv in GNS3 dynamips 0.2.21.	7.5	More Details
CVE-2022-48279	In ModSecurity before 2.9.6 and 3.x before 3.0.8, HTTP multipart requests were incorrectly parsed and could bypass the Web Application Firewall. NOTE: this is related to CVE-2022-39956 but can be considered independent changes to the ModSecurity (C language) codebase.	7.5	More Details
CVE-2022-34460	Prior Dell BIOS versions contain an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21858	Vulnerability in the Oracle Collaborative Planning product of Oracle E-Business Suite (component: Installation). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Collaborative Planning. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Collaborative Planning accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	7.5	More Details
CVE-2023-21857	Vulnerability in the Oracle HCM Common Architecture product of Oracle E-Business Suite (component: Auomated Test Suite). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HCM Common Architecture. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle HCM Common Architecture accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	7.5	More Details
CVE-2023-21856	Vulnerability in the Oracle iSetup product of Oracle E-Business Suite (component: General Ledger Update Transform, Reports). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSetup. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle iSetup accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	7.5	More Details
CVE-2023-21855	Vulnerability in the Oracle Sales for Handhelds product of Oracle E-Business Suite (component: Pocket Outlook Sync(PocketPC)). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Sales for Handhelds. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Sales for Handhelds accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	7.5	More Details
CVE-2023-21854	Vulnerability in the Oracle Sales Offline product of Oracle E-Business Suite (component: Core Components). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Sales Offline. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Sales Offline accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	7.5	More Details
CVE-2023-21853	Vulnerability in the Oracle Mobile Field Service product of Oracle E-Business Suite (component: Synchronization). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Mobile Field Service. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Mobile Field Service accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	7.5	More Details
CVE-2023-21852	Vulnerability in the Oracle Learning Management product of Oracle E-Business Suite (component: Setup). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Learning Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Learning Management accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21851	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Marketing accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	7.5	More Details
CVE-2023-21850	Vulnerability in the Oracle Demantra Demand Management product of Oracle Supply Chain (component: E-Business Collections). Supported versions that are affected are 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Demantra Demand Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Demantra Demand Management accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	7.5	More Details
CVE-2023-21849	Vulnerability in the Oracle Applications DBA product of Oracle E-Business Suite (component: Java utils). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications DBA. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Applications DBA accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	7.5	More Details
CVE-2023-21841	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2023-21842	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2023-21893	Vulnerability in the Oracle Data Provider for .NET component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TCPS to compromise Oracle Data Provider for .NET. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Data Provider for .NET. Note: Applies also to Database client-only on Windows platform. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).	7.5	More Details
CVE-2023-22960	Lexmark products through 2023-01-10 have Improper Control of Interaction Frequency.	7.5	More Details
CVE-2022-32490	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-22655	In Ruckus R310 10.5.1.0.199, Ruckus R500 10.5.1.0.199, Ruckus R600 10.5.1.0.199, Ruckus T300 10.5.1.0.199, Ruckus T301n 10.5.1.0.199, Ruckus T301s 10.5.1.0.199, SmartCell Gateway 200 (SCG200) before 3.6.2.0.795, SmartZone 100 (SZ-100) before 3.6.2.0.795, SmartZone 300 (SZ300) before 3.6.2.0.795, Virtual SmartZone (vSZ) before 3.6.2.0.795, ZoneDirector 1100 9.10.2.0.130, ZoneDirector 1200 10.2.1.0.218, ZoneDirector 3000 10.2.1.0.218, ZoneDirector 5000 10.0.1.0.151, a vulnerability allows attackers to persistently to writing unauthorized image.	7.5	More Details
CVE-2020-22662	In Ruckus R310 10.5.1.0.199, Ruckus R500 10.5.1.0.199, Ruckus R600 10.5.1.0.199, Ruckus T300 10.5.1.0.199, Ruckus T301n 10.5.1.0.199, Ruckus T301s 10.5.1.0.199, SmartCell Gateway 200 (SCG200) before 3.6.2.0.795, SmartZone 100 (SZ-100) before 3.6.2.0.795, SmartZone 300 (SZ300) before 3.6.2.0.795, Virtual SmartZone (vSZ) before 3.6.2.0.795, ZoneDirector 1100 9.10.2.0.130, ZoneDirector 1200 10.2.1.0.218, ZoneDirector 3000 10.2.1.0.218, ZoneDirector 5000 10.0.1.0.151, a vulnerability allows attackers to change and set unauthorized "illegal region code" by remote code Execution command injection which leads to run illegal frequency with maxi output power. Vulnerability allows attacker to create an arbitrary amount of ssid wlans interface per radio which creates overhead over noise (the default max limit is 8 ssid only per radio in solo AP). Vulnerability allows attacker to unlock hidden regions by privilege command injection in WEB GUI.	7.5	More Details
CVE-2023-24021	Incorrect handling of '\0' bytes in file uploads in ModSecurity before 2.9.7 may allow for Web Application Firewall bypasses and buffer over-reads on the Web Application Firewall when executing rules that read the FILES_TMP_CONTENT collection.	7.5	More Details
CVE-2022-38469	An unauthorized user with network access and the decryption key could decrypt sensitive data, such as usernames and passwords.	7.5	More Details
CVE-2020-22656	In Ruckus R310 10.5.1.0.199, Ruckus R500 10.5.1.0.199, Ruckus R600 10.5.1.0.199, Ruckus T300 10.5.1.0.199, Ruckus T301n 10.5.1.0.199, Ruckus T301s 10.5.1.0.199, SmartCell Gateway 200 (SCG200) before 3.6.2.0.795, SmartZone 100 (SZ-100) before 3.6.2.0.795, SmartZone 300 (SZ300) before 3.6.2.0.795, Virtual SmartZone (vSZ) before 3.6.2.0.795, ZoneDirector 1100 9.10.2.0.130, ZoneDirector 1200 10.2.1.0.218, ZoneDirector 3000 10.2.1.0.218, ZoneDirector 5000 10.0.1.0.151, a vulnerability allows attackers to make the Secure Boot in failed attempts state (rfwd).	7.5	More Details
CVE-2020-22659	In Ruckus R310 10.5.1.0.199, Ruckus R500 10.5.1.0.199, Ruckus R600 10.5.1.0.199, Ruckus T300 10.5.1.0.199, Ruckus T301n 10.5.1.0.199, Ruckus T301s 10.5.1.0.199, SmartCell Gateway 200 (SCG200) before 3.6.2.0.795, SmartZone 100 (SZ-100) before 3.6.2.0.795, SmartZone 300 (SZ300) before 3.6.2.0.795, Virtual SmartZone (vSZ) before 3.6.2.0.795, ZoneDirector 1100 9.10.2.0.130, ZoneDirector 1200 10.2.1.0.218, ZoneDirector 3000 10.2.1.0.218, ZoneDirector 5000 10.0.1.0.151, a vulnerability allows attackers to exploit the official image signature to force injection unauthorized image signature.	7.5	More Details
CVE-2022-38112	In DPA 2022.4 and older releases, generated heap memory dumps contain sensitive information in cleartext.	7.5	More Details
CVE-2022-43494	An unauthorized user could be able to read any file on the system, potentially exposing sensitive information.	7.5	More Details
CVE-2022-34393	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34401	Dell BIOS contains a stack based buffer overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to send larger than expected input to a parameter in order to gain arbitrary code execution in SMRAM.	7.5	More Details
CVE-2020-22660	In Ruckus R310 10.5.1.0.199, Ruckus R500 10.5.1.0.199, Ruckus R600 10.5.1.0.199, Ruckus T300 10.5.1.0.199, Ruckus T301n 10.5.1.0.199, Ruckus T301s 10.5.1.0.199, SmartCell Gateway 200 (SCG200) before 3.6.2.0.795, SmartZone 100 (SZ-100) before 3.6.2.0.795, SmartZone 300 (SZ300) before 3.6.2.0.795, Virtual SmartZone (vSZ) before 3.6.2.0.795, ZoneDirector 1100 9.10.2.0.130, ZoneDirector 1200 10.2.1.0.218, ZoneDirector 3000 10.2.1.0.218, ZoneDirector 5000 10.0.1.0.151, a vulnerability allows attackers to force bypass Secure Boot failed attempts and run temporarily the previous Backup image.	7.5	More Details
CVE-2022-34457	Dell command configuration, version 4.8 and prior, contains improper folder permission when installed not to default path but to non-secured path which leads to privilege escalation. This is critical severity vulnerability as it allows non-admin to modify the files inside installed directory and able to make application unavailable for all users.	7.3	More Details
CVE-2023-21894	Vulnerability in the Oracle Global Lifecycle Management NextGen OUI Framework product of Oracle Fusion Middleware (component: NextGen Installer issues). Supported versions that are affected are Prior to 13.9.4.2.11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Global Lifecycle Management NextGen OUI Framework executes to compromise Oracle Global Lifecycle Management NextGen OUI Framework. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Global Lifecycle Management NextGen OUI Framework. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H).	7.3	More Details
CVE-2023-24059	Grand Theft Auto V for PC allows attackers to achieve partial remote code execution or modify files on a PC, as exploited in the wild in January 2023.	7.3	More Details
CVE-2022-4323	The Analyticator WordPress plugin before 6.5.6 unserializes user input provided via the settings, which could allow high privilege users such as admin to perform PHP Object Injection when a suitable gadget is present	7.2	More Details
CVE-2022-3425	The Analyticator WordPress plugin before 6.5.6 unserializes user input provided via the settings, which could allow high-privilege users such as admin to perform PHP Object Injection when a suitable gadget is present.	7.2	More Details
CVE-2023-24040	dtprintinfo in Common Desktop Environment 1.6 has a bug in the parser of lpstat (an invoked external command) during listing of the names of available printers. This allows low-privileged local users to inject arbitrary printer names via the $HOME/.printers file. This injection allows those users to manipulate the control flow and disclose memory contents on Solaris 10 systems. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	7.1	More Details
CVE-2023-23690	Cloud Mobility for Dell EMC Storage, versions 1.3.0.X and below contains an Improper Check for Certificate Revocation vulnerability. A threat actor does not need any specific privileges to potentially exploit this vulnerability. An attacker could perform a man-in-the-middle attack and eavesdrop on encrypted communications from Cloud Mobility to Cloud Storage devices. Exploitation could lead to the compromise of secret and sensitive information, cloud storage connection downtime, and the integrity of the connection to the Cloud devices.	7.0	More Details
CVE-2022-48191	A vulnerability exists in Trend Micro Maximum Security 2022 (17.7) wherein a low-privileged user can write a known malicious executable to a specific location and in the process of removal and restoral an attacker could replace an original folder with a mount point to an arbitrary location, allowing a escalation of privileges on an affected system.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47917	Sewio's Real-Time Location System (RTLS) Studio version 2.0.0 up to and including version 2.6.2 is vulnerable to improper input validation of user input to several modules and services of the software. This could allow an attacker to delete arbitrary files and cause a denial-of-service condition.	6.8	More Details
CVE-2020-22007	OS Command Injection vulnerability in OKER G955V1 v1.03.02.20161128, allows physical attackers to interrupt the boot sequence and execute arbitrary commands with root privileges.	6.8	More Details
CVE-2023-20043	A vulnerability in Cisco CX Cloud Agent of could allow an authenticated, local attacker to elevate their privileges. This vulnerability is due to insecure file permissions. An attacker could exploit this vulnerability by calling the script with sudo. A successful exploit could allow the attacker to take complete control of the affected device.	6.7	More Details
CVE-2023-20044	A vulnerability in Cisco CX Cloud Agent of could allow an authenticated, local attacker to elevate their privileges. This vulnerability is due to insecure file permissions. An attacker could exploit this vulnerability by persuading support to update settings which call the insecure script. A successful exploit could allow the attacker to take complete control of the affected device.	6.7	More Details
CVE-2022-3430	A potential vulnerability in the WMI Setup driver on some consumer Lenovo Notebook devices may allow an attacker with elevated privileges to modify secure boot setting by modifying an NVRAM variable.	6.7	More Details
CVE-2023-23824	Auth. SQL Injection (SQLi) vulnerability in WP-TopBar <= 5.36 versions.	6.7	More Details
CVE-2023-20026	A vulnerability in the web-based management interface of Cisco Small Business Routers RV042 Series could allow an authenticated, remote attacker to inject arbitrary commands on an affected device. This vulnerability is due to improper validation of user input fields within incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device with root-level privileges. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device.	6.5	More Details
CVE-2023-0398	Cross-Site Request Forgery (CSRF) in GitHub repository modoboa/modoboa prior to 2.0.4.	6.5	More Details
CVE-2023-23687	Auth. Stored Cross-Site Scripting (XSS) vulnerability in Youtube shortcode <= 1.8.5 versions.	6.5	More Details
CVE-2020-22661	In Ruckus R310 10.5.1.0.199, Ruckus R500 10.5.1.0.199, Ruckus R600 10.5.1.0.199, Ruckus T300 10.5.1.0.199, Ruckus T301n 10.5.1.0.199, Ruckus T301s 10.5.1.0.199, SmartCell Gateway 200 (SCG200) before 3.6.2.0.795, SmartZone 100 (SZ-100) before 3.6.2.0.795, SmartZone 300 (SZ300) before 3.6.2.0.795, Virtual SmartZone (vSZ) before 3.6.2.0.795, ZoneDirector 1100 9.10.2.0.130, ZoneDirector 1200 10.2.1.0.218, ZoneDirector 3000 10.2.1.0.218, ZoneDirector 5000 10.0.1.0.151, a vulnerability allows attackers to erase the backup secondary official image and write secondary backup unauthorized image.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20047	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature of Cisco Webex Room Phone and Cisco Webex Share devices could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient resource allocation. An attacker could exploit this vulnerability by sending crafted LLDP traffic to an affected device. A successful exploit could allow the attacker to exhaust the memory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart.	6.5	More Details
CVE-2023-21719	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	6.5	More Details
CVE-2023-0438	Cross-Site Request Forgery (CSRF) in GitHub repository modoboa/modoboa prior to 2.0.4.	6.5	More Details
CVE-2022-47950	An issue was discovered in OpenStack Swift before 2.28.1, 2.29.x before 2.29.2, and 2.30.0. By supplying crafted XML files, an authenticated user may coerce the S3 API into returning arbitrary file contents from the host server, resulting in unauthorized read access to potentially sensitive data. This impacts both s3api deployments (Rocky or later), and swift3 deployments (Queens and earlier, no longer actively developed).	6.5	More Details
CVE-2021-37498	An SSRF issue was discovered in Reprise License Manager (RLM) web interface through 14.2BL4 that allows remote attackers to trigger outbound requests to intranet servers, conduct port scans via the actserver parameter in License Activation function.	6.5	More Details
CVE-2021-37499	CRLF vulnerability in Reprise License Manager (RLM) web interface through 14.2BL4 in the password parameter in View License Result function, that allows remote attackers to inject arbitrary HTTP headers.	6.5	More Details
CVE-2022-4443	The BruteBank WordPress plugin before 1.9 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged-in admin change them via a CSRF attack.	6.5	More Details
CVE-2023-22721	Auth. Stored Cross-Site Scripting (XSS) in Oi Yandex.Maps for WordPress <= 3.2.7 versions.	6.5	More Details
CVE-2022-4548	The Optimize images ALT Text & names for SEO using AI WordPress plugin before 2.0.8 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged-in admin change them via a CSRF attack.	6.5	More Details
CVE-2022-47015	MariaDB Server before 10.3.34 thru 10.9.3 is vulnerable to Denial of Service. It is possible for function spider_db_mbase::print_warnings to dereference a null pointer.	6.5	More Details
CVE-2022-31901	Buffer overflow in function Notepad_plus::addHotSpot in Notepad++ v8.4.3 and earlier allows attackers to crash the application via two crafted files.	6.5	More Details
CVE-2022-45103	Dell Unisphere for PowerMax vApp, VASA Provider vApp, and Solution Enabler vApp version 9.2.3.x contain an information disclosure vulnerability. A low privileged remote attacker could potentially exploit this vulnerability, leading to read arbitrary files on the underlying file system.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47881	Foxit PDF Reader and PDF Editor 11.2.1.53537 and earlier has an Out-of-Bounds Read vulnerability.	6.5	More Details
CVE-2023-21868	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2022-41505	An access control issue on TP-LInk Tapo C200 V1 devices allows physically proximate attackers to obtain root access by connecting to the UART pins, interrupting the boot process, and setting an init=/bin/sh value.	6.4	More Details
CVE-2023-22745	tpm2-tss is an open source software implementation of the Trusted Computing Group (TCG) Trusted Platform Module (TPM) 2 Software Stack (TSS2). In affected versions `Tss2_RC_SetHandler` and `Tss2_RC_Decode` both index into `layer_handler` with an 8 bit layer number, but the array only has `TPM2_ERROR_TSS2_RC_LAYER_COUNT` entries, so trying to add a handler for higher-numbered layers or decode a response code with such a layer number reads/writes past the end of the buffer. This Buffer overrun, could result in arbitrary code execution. An example attack would be a MiTM bus attack that returns 0xFFFFFFFF for the RC. Given the common use case of TPM modules an attacker must have local access to the target machine with local system privileges which allows access to the TPM system. Usually TPM access requires administrative privilege.	6.4	More Details
CVE-2022-20964	A vulnerability in the web-based management interface of Cisco Identity Services Engine could allow an authenticated, remote attacker to inject arbitrary commands on the underlying operating system. This vulnerability is due to improper validation of user input within requests as part of the web-based management interface. An attacker could exploit this vulnerability by manipulating requests to the web-based management interface to contain operating system commands. A successful exploit could allow the attacker to execute arbitrary operating system commands on the underlying operating system with the privileges of the web services user. Cisco has not yet released software updates that address this vulnerability.	6.3	More Details
CVE-2023-21860	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: Internal Operations). Supported versions that are affected are 7.4.38 and prior, 7.5.28 and prior, 7.6.24 and prior and 8.0.31 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	6.3	More Details
CVE-2022-46733	Sewio’s Real-Time Location System (RTLS) Studio version 2.0.0 up to and including version 2.6.2 is vulnerable to cross-site scripting in its backup services. An attacker could take advantage of this vulnerability to execute arbitrary commands.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21829	Vulnerability in the Oracle Database RDBMS Security component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Oracle Database RDBMS Security. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Database RDBMS Security accessible data as well as unauthorized read access to a subset of Oracle Database RDBMS Security accessible data. CVSS 3.1 Base Score 6.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:N).	6.3	More Details
CVE-2015-10070	A vulnerability was found in copperwall Twiddit. It has been rated as critical. This issue affects some unknown processing of the file index.php. The manipulation leads to sql injection. The identifier of the patch is 2203d4ce9810bdaccece5c48ff4888658a01acfc. It is recommended to apply a patch to fix this issue. The identifier VDB-218897 was assigned to this vulnerability.	6.3	More Details
CVE-2022-4816	A denial-of-service vulnerability has been identified in Lenovo Safecenter that could allow a local user to crash the application.	6.2	More Details
CVE-2022-47990	IBM AIX 7.1, 7.2, 7.3 and VIOS , 3.1 could allow a non-privileged local user to exploit a vulnerability in X11 to cause a buffer overflow that could result in a denial of service or arbitrary code execution. IBM X-Force ID: 243556.	6.2	More Details
CVE-2023-23010	Cross Site Scripting (XSS) vulnerability in Ecommerce-CodeIgniter-Bootstrap thru commit d5904379ca55014c5df34c67deda982c73dc7fe5 (on Dec 27, 2022), allows attackers to execute arbitrary code via the languages and trans_load parameters in file add_product.php.	6.1	More Details
CVE-2023-23014	Cross Site Scripting (XSS) vulnerability in InventorySystem thru commit e08fbbe17902146313501ed0b5feba81d58f455c (on Apr 23, 2021) via edit_store_name and edit_active inputs in file InventorySystem.php.	6.1	More Details
CVE-2022-41441	Multiple cross-site scripting (XSS) vulnerabilities in ReQlogic v11.3 allow attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the POBatch and WaitDuration parameters.	6.1	More Details
CVE-2023-20058	A vulnerability in the web-based management interface of Cisco Unified Intelligence Center could allow an unauthenticated, remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.	6.1	More Details
CVE-2023-24044	A Host Header Injection issue on the Login page of Plesk Obsidian through 18.0.49 allows attackers to redirect users to malicious websites via a Host request header. NOTE: the vendor's position is "the ability to use arbitrary domain names to access the panel is an intended feature."	6.1	More Details
CVE-2023-24026	In MISP 2.4.167, app/webroot/js/event-graph.js has an XSS vulnerability via an event-graph preview payload.	6.1	More Details
CVE-2022-45537	EyouCMS <= 1.6.0 was discovered a reflected-XSS in the article publish component in cookie "ENV_LIST_URL".	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23491	The Quick Event Manager WordPress Plugin, version < 9.7.5, is affected by a reflected cross-site scripting vulnerability in the 'category' parameter of its 'qem_ajax_calendar' action.	6.1	More Details
CVE-2022-45538	EyouCMS <= 1.6.0 was discovered a reflected-XSS in the article publish component in cookie "ENV_GOBACK_URL".	6.1	More Details
CVE-2023-23012	Cross Site Scripting (XSS) vulnerability in craigrodway classroombookings 2.6.4 allows attackers to execute arbitrary code or other unspecified impacts via the input bgcol in file Weeks.php.	6.1	More Details
CVE-2022-45539	EyouCMS <= 1.6.0 was discovered a reflected-XSS in FileManager component in GET value "activepath" when creating a new file.	6.1	More Details
CVE-2022-45540	EyouCMS <= 1.6.0 was discovered a reflected-XSS in article type editor component in POST value "name" if the value contains a malformed UTF-8 char.	6.1	More Details
CVE-2022-45541	EyouCMS <= 1.6.0 was discovered a reflected-XSS in the article attribute editor component in POST value "value" if the value contains a non-integer char.	6.1	More Details
CVE-2022-45557	Cross site scripting (XSS) vulnerability in Hundredrabbits Left 7.1.5 for MacOS allows attackers to execute arbitrary code via file names.	6.1	More Details
CVE-2022-45558	Cross site scripting (XSS) vulnerability in Hundredrabbits Left 7.1.5 for MacOS allows attackers to execute arbitrary code via the meta tag.	6.1	More Details
CVE-2023-24027	In MISP 2.4.167, app/webroot/js/action_table.js allows XSS via a network history name.	6.1	More Details
CVE-2023-20019	A vulnerability in the web-based management interface of Cisco BroadWorks Application Delivery Platform, Cisco BroadWorks Application Server, and Cisco BroadWorks Xtended Services Platform could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	6.1	More Details
CVE-2023-0410	Cross-site Scripting (XSS) - Generic in GitHub repository builderio/qwik prior to 0.1.0-beta5.	6.1	More Details
CVE-2023-23015	Cross Site Scripting (XSS) vulnerability in Kalkun 0.8.0 via username input in file User_model.php.	6.1	More Details
CVE-2023-23024	Book Store Management System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in /bsms_ci/index.php/book. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the writer parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0214	A cross-site scripting vulnerability in Skyhigh SWG in main releases 11.x prior to 11.2.6, 10.x prior to 10.2.17, and controlled release 12.x prior to 12.0.1 allows a remote attacker to craft SWG-specific internal requests with URL paths to any third-party website, causing arbitrary content to be injected into the response when accessed through SWG.	6.1	More Details
CVE-2022-46888	Multiple reflective cross-site scripting (XSS) vulnerabilities in NexusPHP before 1.7.33 allow remote attackers to inject arbitrary web script or HTML via the secret parameter in /login.php; q parameter in /user-ban-log.php; query parameter in /log.php; text parameter in /moresmiles.php; q parameter in myhr.php; or id parameter in /viewrequests.php.	6.1	More Details
CVE-2023-24070	app/View/AuthKeys/authkey_display.ctp in MISP through 2.4.167 has an XSS in authkey add via a Referer field.	6.1	More Details
CVE-2021-43446	ONLYOFFICE all versions as of 2021-11-08 is vulnerable to Cross Site Scripting (XSS). The "macros" feature of the document editor allows malicious cross site scripting payloads to be used.	6.1	More Details
CVE-2022-4307	The پلاگین پرداخت دلخواه WordPress plugin before 2.9.3 does not sanitise and escape some parameters, allowing unauthenticated attackers to send a request with XSS payloads, which will be triggered when a high privilege users such as admin visits a page from the plugin.	6.1	More Details
CVE-2022-43704	The Sinilink XY-WFT1 WiFi Remote Thermostat, running firmware 1.3.6, allows an attacker to bypass the intended requirement to communicate using MQTT. It is possible to replay Sinilink aka SINILINK521 protocol (udp/1024) commands interfacing directly with the target device. This, in turn, allows for an attack to control the onboard relay without requiring authentication via the mobile application. This might result in an unacceptable temperature within the target device's physical environment.	5.9	More Details
CVE-2023-22863	IBM Robotic Process Automation 20.12.0 through 21.0.2 defaults to HTTP in some RPA commands when the prefix is not explicitly specified in the URL. This could allow an attacker to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 244109.	5.9	More Details
CVE-2022-40267	Predictable Seed in Pseudo-Random Number Generator (PRNG) vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U-xMy/z (x=32,64,80, y=T,R, z=ES,DS,ESS,DSS) with serial number 17X**** or later, and versions 1.280 and prior, Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U-xMy/z (x=32,64,80, y=T,R, z=ES,DS,ESS,DSS) with serial number 179**** and prior, and versions 1.074 and prior, Mitsubishi Electric Corporation MELSEC iQ-F Series FX5UC-xMy/z (x=32,64,96, y=T, z=D,DSS)) with serial number 17X**** or later, and versions 1.280 and prior, Mitsubishi Electric Corporation MELSEC iQ-F Series FX5UC-xMy/z (x=32,64,96, y=T, z=D,DSS)) with serial number 179**** and prior, and versions 1.074 and prior, Mitsubishi Electric Corporation MELSEC iQ-F Series FX5UC-32MT/DS-TS versions 1.280 and prior, Mitsubishi Electric Corporation MELSEC iQ-F Series FX5UC-32MT/DSS-TS versions 1.280 and prior, Mitsubishi Electric Corporation MELSEC iQ-F Series FX5UJ-xMy/z (x=24,40,60, y=T,R, z=ES,ESS) versions 1.042 and prior, Mitsubishi Electric Corporation MELSEC iQ-F Series FX5UJ-xMy/ES-A (x=24,40,60, y=T,R) versions 1.043 and prior, Mitsubishi Electric Corporation MELSEC iQ-F Series FX5S-xMy/z (x=30,40,60,80, y=T,R, z=ES,ESS) versions 1.003 and prior, Mitsubishi Electric Corporation MELSEC iQ-F Series FX5UC-32MR/DS-TS versions 1.280 and prior, Mitsubishi Electric Corporation MELSEC iQ-R Series R00/01/02CPU versions 33 and prior, Mitsubishi Electric Corporation MELSEC iQ-R Series R04/08/16/32/120(EN)CPU versions 66 and prior allows a remote unauthenticated attacker to access the Web server function by guessing the random numbers used for authentication from several used random numbers.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21875	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.31 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H).	5.9	More Details
CVE-2022-3738	The vulnerability allows a remote unauthenticated attacker to download a backup file, if one exists. That backup file might contain sensitive information like credentials and cryptographic material. A valid user has to create a backup after the last reboot for this attack to be successfull.	5.9	More Details
CVE-2022-39167	IBM Spectrum Virtualize 8.5, 8.4, 8.3, 8.2, and 7.8, under certain configurations, could disclose sensitive information to an attacker using man-in-the-middle techniques. IBM X-Force ID: 235408.	5.9	More Details
CVE-2022-3100	A flaw was found in the openstack-barbican component. This issue allows an access policy bypass via a query string when accessing the API.	5.9	More Details
CVE-2017-20174	A vulnerability was found in bastianallgeier Kirby Webmentions Plugin and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to injection. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The patch is identified as 55bedea78ae9af916a9a41497bd9996417851502. It is recommended to apply a patch to fix this issue. VDB-218894 is the identifier assigned to this vulnerability.	5.6	More Details
CVE-2020-36651	A vulnerability has been found in youngerheart nodeserver and classified as critical. Affected by this vulnerability is an unknown functionality of the file nodeserver.js. The manipulation leads to path traversal. The identifier of the patch is c4c0f0138ab5afbac58e03915d446680421bde28. It is recommended to apply a patch to fix this issue. The identifier VDB-218461 was assigned to this vulnerability.	5.5	More Details
CVE-2015-10068	A vulnerability classified as critical was found in danynab movify-j. This vulnerability affects the function getByMovieId of the file app/business/impl/ReviewServiceImpl.java. The manipulation of the argument movieId/username leads to sql injection. The name of the patch is c3085e01936a4d7eff1eda3093f25d56cc4d2ec5. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-218476.	5.5	More Details
CVE-2010-10007	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in lierdakil click-reminder. It has been rated as critical. This issue affects the function db_query of the file src/backend/include/BaseAction.php. The manipulation leads to sql injection. The identifier of the patch is 41213b660e8eb01b22c8074f06208f59a73ca8dc. It is recommended to apply a patch to fix this issue. The identifier VDB-218465 was assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	5.5	More Details
CVE-2022-1109	An incorrect default permissions vulnerability in Lenovo Leyun cloud music application could allow denial of service.	5.5	More Details
CVE-2023-24055	KeePass through 2.53 (in a default installation) allows an attacker, who has write access to the XML configuration file, to obtain the cleartext passwords by adding an export trigger. NOTE: the vendor's position is that the password database is not intended to be secure against an attacker who has that level of access to the local PC.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43455	Sewio's Real-Time Location System (RTLS) Studio version 2.0.0 up to and including version 2.6.2 is vulnerable to improper input validation of user input to the service_start, service_stop, and service_restart modules of the software. This could allow an attacker to start, stop, or restart arbitrary services running on the server.	5.5	More Details
CVE-2023-24056	In pkgconf through 1.9.3, variable duplication can cause unbounded string expansion due to incorrect checks in libpkgconf/tuple.c:pkgconf_tuple_parse. For example, a .pc file containing a few hundred bytes can expand to one billion bytes.	5.5	More Details
CVE-2023-23144	Integer overflow vulnerability in function Q_DecCoordOnUnitSphere file bifs/unquantize.c in GPAC version 2.2-rev0-gab012bbfb-master.	5.5	More Details
CVE-2023-21899	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: Applies to VirtualBox VMs running Windows 7 and later. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	5.5	More Details
CVE-2023-21898	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: Applies to VirtualBox VMs running Windows 7 and later. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	5.5	More Details
CVE-2022-35977	Redis is an in-memory database that persists on disk. Authenticated users issuing specially crafted `SETRANGE` and `SORT(_RO)` commands can trigger an integer overflow, resulting with Redis attempting to allocate impossible amounts of memory and abort with an out-of-memory (OOM) panic. The problem is fixed in Redis versions 7.0.8, 6.2.9 and 6.0.17. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.5	More Details
CVE-2017-20172	A vulnerability was found in ridhoq soundslike. It has been classified as critical. Affected is the function get_song_relations of the file app/api/songs.py. The manipulation leads to sql injection. The patch is identified as 90bb4fb667d9253d497b619b9adaac83bf0ce0f8. It is recommended to apply a patch to fix this issue. VDB-218490 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2023-21880	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21877	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	5.5	More Details
CVE-2023-21872	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	5.5	More Details
CVE-2023-21869	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	5.5	More Details
CVE-2023-22458	Redis is an in-memory database that persists on disk. Authenticated users can issue a `HRANDFIELD` or `ZRANDMEMBER` command with specially crafted arguments to trigger a denial-of-service by crashing Redis with an assertion failure. This problem affects Redis versions 6.2 or newer up to but not including 6.2.9 as well as versions 7.0 up to but not including 7.0.8. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.5	More Details
CVE-2023-0446	The My YouTube Channel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via its settings parameters in versions up to, and including, 3.0.12.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.5	More Details
CVE-2015-10066	A vulnerability was found in tynx wuersch and classified as critical. Affected by this issue is the function packValue/getByCustomQuery of the file backend/base/Store.class.php. The manipulation leads to sql injection. The patch is identified as 66d4718750a741d1053d327a79e285fd50372519. It is recommended to apply a patch to fix this issue. VDB-218462 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2021-33642	When a file is processed, an infinite loop occurs in next_inline() of the more_curly() function.	5.5	More Details
CVE-2023-21613	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21614	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-20040	A vulnerability in the NETCONF service of Cisco Network Services Orchestrator (NSO) could allow an authenticated, remote attacker to cause a denial of service (DoS) on an affected system that is running as the root user. To exploit this vulnerability, the attacker must be a member of the admin group. This vulnerability exists because user-supplied input is not properly validated when NETCONF is used to upload packages to an affected device. An attacker could exploit this vulnerability by uploading a specially crafted package file. A successful exploit could allow the attacker to write crafted files to arbitrary locations on the filesystem or delete arbitrary files from the filesystem of an affected device, resulting in a DoS condition. Note: By default, during install, Cisco NSO will be set up to run as the root user unless the --run-as-user option is used.	5.5	More Details
CVE-2015-10069	A vulnerability was found in viakondratiuk cash-machine. It has been declared as critical. This vulnerability affects the function is_card_pin_at_session/update_failed_attempts of the file machine.py. The manipulation leads to sql injection. The name of the patch is 62a6e24efdfa195b70d7df140d8287fdc38eb66d. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-218896.	5.5	More Details
CVE-2011-10001	A vulnerability was found in iamdroppy phoenixcf. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file content/2-Community/articles.cfm. The manipulation leads to sql injection. The patch is named d156faf8bc36cd49c3b10d3697ef14167ad451d8. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218491.	5.5	More Details
CVE-2023-21585	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-21581	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2013-10014	A vulnerability classified as critical has been found in oktora24 2moons. Affected is an unknown function. The manipulation leads to sql injection. The patch is identified as 1b09cf7672eb85b5b0c8a4de321f7a4ad87b09a7. It is recommended to apply a patch to fix this issue. VDB-218898 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2023-21603	Adobe Dimension version 3.4.6 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-21601	Adobe Dimension version 3.4.6 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2014-125083	A vulnerability has been found in Anant Labs google-enterprise-connector-dctm up to 3.2.3 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation of the argument username/domain leads to sql injection. The patch is named 6fba04f18ab7764002a1da308e7cd9712b501cb7. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218911.	5.5	More Details
CVE-2010-10009	A vulnerability was found in frioux ptome. It has been rated as critical. This issue affects some unknown processing. The manipulation leads to sql injection. The patch is named 26829bba67858ca0bd4ce49ad50e7ce653914276. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218519.	5.5	More Details
CVE-2022-48281	processCropSelections in tools/tiffcrop.c in LibTIFF through 4.5.0 has a heap-based buffer overflow (e.g., "WRITE of size 307203") via a crafted TIFF image.	5.5	More Details
CVE-2017-20173	A vulnerability was found in AlexRed contentmap. It has been rated as critical. Affected by this issue is the function Load of the file contentmap.php. The manipulation of the argument contentid leads to sql injection. The name of the patch is dd265d23ff4abac97422835002c6a47f45ae2a66. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-218492.	5.5	More Details
CVE-2012-10006	A vulnerability classified as critical has been found in ale7714 sigeprosi. This affects an unknown part. The manipulation leads to sql injection. The identifier of the patch is 5291886f6c992316407c376145d331169c55f25b. It is recommended to apply a patch to fix this issue. The identifier VDB-218493 was assigned to this vulnerability.	5.5	More Details
CVE-2014-125082	A vulnerability was found in nivit redports. It has been declared as critical. This vulnerability affects unknown code of the file redports-trac/redports/model.py. The manipulation leads to sql injection. The name of the patch is fc2c1ea1b8d795094abb15ac73cab90830534e04. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-218464.	5.5	More Details
CVE-2022-4474	The Easy Social Feed WordPress plugin before 6.4.0 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 admin.	5.4	More Details
CVE-2022-4758	The 10WebMapBuilder WordPress plugin before 1.0.72 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-2022-4760	The OneClick Chat to Order WordPress plugin before 1.0.4.2 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-2022-4775	The GeoDirectory WordPress plugin before 2.2.22 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-2022-4545	The Sitemap WordPress plugin before 4.4 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-2022-4467	The Search & Filter WordPress plugin before 1.2.16 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 admin.	5.4	More Details
CVE-2022-4789	The WPZOOM Portfolio WordPress plugin before 1.2.2 does not validate and escape one of its shortcode attributes, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attack.	5.4	More Details
CVE-2022-4790	The WP Google My Business Auto Publish WordPress plugin before 3.4 does not validate and escape one of its shortcode attributes, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attack.	5.4	More Details
CVE-2022-4832	The Store Locator WordPress plugin before 1.4.9 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-2022-4751	The Word Balloon WordPress plugin before 4.19.3 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-2021-24837	The Passster WordPress plugin before 3.5.5.8 does not escape the area parameter of its shortcode, which could allow users with a role as low as Contributor to perform Cross-Site Scripting attacks.	5.4	More Details
CVE-2022-40034	Cross-Site Scripting (XSS) vulnerability found in Rawchen blog-ssm v1.0 allows attackers to execute arbitrary code via the 'notifyInfo' parameter.	5.4	More Details
CVE-2022-4753	The Print-O-Matic WordPress plugin before 2.1.8 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-2022-4475	The Collapse-O-Matic WordPress plugin before 1.8.3 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 admin.	5.4	More Details
CVE-2022-4718	The Landing Page Builder WordPress plugin before 1.4.9.9 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-2022-4716	The WP Popups WordPress plugin before 2.1.4.8 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-2022-4570	The Top 10 WordPress plugin before 3.2.3 does not validate and escape some of its Block 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-2022-4576	The Easy Bootstrap Shortcode WordPress plugin through 4.5.4 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-2022-4542	The Compact WP Audio Player WordPress plugin before 1.9.8 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-2022-4509	The Content Control WordPress plugin before 1.1.10 does not validate and escapes some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as a contributor to perform Stored Cross-Site Scripting attacks, which could be used against high privilege users such as admins.	5.4	More Details
CVE-2022-4625	The Login Logout Menu WordPress plugin before 1.4.0 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-2022-4627	The ShiftNav WordPress plugin before 1.7.2 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-2022-4629	The Product Slider for WooCommerce WordPress plugin before 2.6.4 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-2022-4650	The HashBar WordPress plugin before 1.3.6 does not validate and escape one of its shortcode attributes, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attack.	5.4	More Details
CVE-2022-4668	The Easy Appointments WordPress plugin before 3.11.2 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-2022-4672	The WordPress Simple Shopping Cart WordPress plugin before 4.6.2 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-2022-4485	The Page-list WordPress plugin before 5.3 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-2022-4673	The Rate my Post WordPress plugin before 3.3.9 does not validate and escape one of its shortcode attributes, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attack.	5.4	More Details
CVE-2022-4675	The Mongoose Page Plugin WordPress plugin before 1.9.0 does not validate and escape one of its shortcode attributes, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attack.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4706	The Genesis Columns Advanced WordPress plugin before 2.0.4 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 a contributor to perform Stored Cross-Site Scripting attacks which could be used against high-privilege users such as admins.	5.4	More Details
CVE-2022-4715	The Structured Content WordPress plugin before 1.5.1 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-2022-4624	The GS Logo Slider WordPress plugin before 3.3.8 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-2022-4554	B2B Customer Ordering System developed by ID Software Project and Consultancy Services before version 1.0.0.347 has an authenticated Reflected XSS vulnerability. This has been fixed in the version 1.0.0.347.	5.4	More Details
CVE-2023-21845	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Panel Processor). The supported version that is affected is 8.60. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	5.4	More Details
CVE-2022-20966	A vulnerability in the web-based management interface of Cisco Identity Services Engine could allow an authenticated, remote attacker to conduct cross-site scripting attacks against other users of the application web-based management interface. This vulnerability is due to improper validation of input to an application feature before storage within the web-based management interface. An attacker could exploit this vulnerability by creating entries within the application interface that contain malicious HTML or script code. A successful exploit could allow the attacker to store malicious HTML or script code within the application interface for use in further cross-site scripting attacks. Cisco has not yet released software updates that address this vulnerability.	5.4	More Details
CVE-2023-22373	Cross-site scripting vulnerability in CONPROSYS HMI System (CHS) Ver.3.4.5 and earlier allows a remote authenticated attacker to inject an arbitrary script and obtain the sensitive information.	5.4	More Details
CVE-2022-46889	A persistent cross-site scripting (XSS) vulnerability in NexusPHP before 1.7.33 allows remote authenticated attackers to permanently inject arbitrary web script or HTML via the title parameter used in /subtitles.php.	5.4	More Details
CVE-2022-47197	An insecure default vulnerability exists in the Post Creation functionality of Ghost Foundation Ghost 5.9.4. Default installations of Ghost allow non-administrator users to inject arbitrary Javascript in posts, which allow privilege escalation to administrator via XSS. To trigger this vulnerability, an attacker can send an HTTP request to inject Javascript in a post to trick an administrator into visiting the post.A stored XSS vulnerability exists in the `codeinjection_foot` for a post.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47196	An insecure default vulnerability exists in the Post Creation functionality of Ghost Foundation Ghost 5.9.4. Default installations of Ghost allow non-administrator users to inject arbitrary Javascript in posts, which allow privilege escalation to administrator via XSS. To trigger this vulnerability, an attacker can send an HTTP request to inject Javascript in a post to trick an administrator into visiting the post.A stored XSS vulnerability exists in the `codeinjection_head` for a post.	5.4	More Details
CVE-2022-47195	An insecure default vulnerability exists in the Post Creation functionality of Ghost Foundation Ghost 5.9.4. Default installations of Ghost allow non-administrator users to inject arbitrary Javascript in posts, which allow privilege escalation to administrator via XSS. To trigger this vulnerability, an attacker can send an HTTP request to inject Javascript in a post to trick an administrator into visiting the post.A stored XSS vulnerability exists in the `facebook` field for a user.	5.4	More Details
CVE-2023-21888	Vulnerability in the Primavera Gateway product of Oracle Construction and Engineering (component: WebUI). Supported versions that are affected are 18.8.0-18.8.15, 19.12.0-19.12.15, 20.12.0-20.12.10 and 21.12.0-21.12.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera Gateway. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera Gateway, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera Gateway accessible data as well as unauthorized read access to a subset of Primavera Gateway accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2022-47194	An insecure default vulnerability exists in the Post Creation functionality of Ghost Foundation Ghost 5.9.4. Default installations of Ghost allow non-administrator users to inject arbitrary Javascript in posts, which allow privilege escalation to administrator via XSS. To trigger this vulnerability, an attacker can send an HTTP request to inject Javascript in a post to trick an administrator into visiting the post.A stored XSS vulnerability exists in the `twitter` field for a user.	5.4	More Details
CVE-2023-21891	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Visual Analyzer). Supported versions that are affected are 5.9.0.0.0 and 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2023-21892	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Visual Analyzer). Supported versions that are affected are 5.9.0.0.0 and 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21844	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Elastic Search). Supported versions that are affected are 8.59 and 8.60. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2022-45613	Book Store Management System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in /bsms_ci/index.php/book. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the publisher parameter.	5.4	More Details
CVE-2022-45542	EyouCMS <= 1.6.0 was discovered a reflected-XSS in the FileManager component in GET parameter "filename" when editing any file.	5.4	More Details
CVE-2023-0404	The Events Made Easy plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on several functions related to AJAX actions in versions up to, and including, 2.3.16. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to invoke those functions intended for administrator use. While the plugin is still pending review from the WordPress repository, site owners can download a copy of the patched version directly from the developer's Github at https://github.com/liedekef/events-made-easy	5.4	More Details
CVE-2023-0403	The Social Warfare plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.4.0. This is due to missing or incorrect nonce validation on several AJAX actions. This makes it possible for unauthenticated attackers to delete post meta information and reset network access tokens, via forged request granted they can trick a site administrator into performing an action such as clicking on a link.	5.4	More Details
CVE-2023-0402	The Social Warfare plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on several AJAX actions in versions up to, and including, 4.3.0. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to delete post meta information and reset network access tokens.	5.4	More Details
CVE-2021-27782	HCL BigFix Mobile / Modern Client Management Admin and Config UI passwords can be brute-forced. User should be locked out for multiple invalid attempts.	5.4	More Details
CVE-2022-4235	RushBet version 2022.23.1-b490616d allows a remote attacker to steal customer accounts via use of a malicious application. This is possible because the application exposes an activity and does not properly validate the data it receives.	5.4	More Details
CVE-2023-22910	An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. There is XSS in Wikibase date formatting via wikibase-time-precision-* fields. This allows JavaScript execution by staff/admin users who do not intentionally have the editsitejs capability.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21847	Vulnerability in the Oracle Web Applications Desktop Integrator product of Oracle E-Business Suite (component: Download). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Web Applications Desktop Integrator. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Web Applications Desktop Integrator, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Web Applications Desktop Integrator accessible data as well as unauthorized read access to a subset of Oracle Web Applications Desktop Integrator accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2023-20037	A vulnerability in Cisco Industrial Network Director could allow an authenticated, remote attacker to conduct stored cross-site scripting (XSS) attacks. The vulnerability is due to improper validation of content submitted to the affected application. An attacker could exploit this vulnerability by sending requests containing malicious values to the affected system. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	5.4	More Details
CVE-2023-21861	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Visual Analyzer). Supported versions that are affected are 5.9.0.0.0 and 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2022-38110	In Database Performance Analyzer (DPA) 2022.4 and older releases, certain URL vectors are susceptible to authenticated reflected cross-site scripting.	5.4	More Details
CVE-2023-21835	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via DTLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21830	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf; Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).	5.3	More Details
CVE-2023-0440	Observable Discrepancy in GitHub repository healthchecks/healthchecks prior to v2.6.	5.3	More Details
CVE-2023-21831	Vulnerability in the PeopleSoft Enterprise CS Academic Advisement product of Oracle PeopleSoft (component: Advising Notes). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise CS Academic Advisement. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise CS Academic Advisement accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2021-43448	ONLYOFFICE all versions as of 2021-11-08 is vulnerable to Improper Input Validation. A lack of input validation can allow an attacker to spoof the names of users who interact with a document, if the document id is known.	5.3	More Details
CVE-2023-21825	Vulnerability in the Oracle iSupplier Portal product of Oracle E-Business Suite (component: Supplier Management). Supported versions that are affected are 12.2.6-12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSupplier Portal. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle iSupplier Portal accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2022-25901	Versions of the package cookiejar before 2.1.4 are vulnerable to Regular Expression Denial of Service (ReDoS) via the Cookie.parse function, which uses an insecure regular expression.	5.3	More Details
CVE-2023-22485	cmark-gfm is GitHub's fork of cmark, a CommonMark parsing and rendering library and program in C. In versions prior 0.29.0.gfm.7, a crafted markdown document can trigger an out-of-bounds read in the `validate_protocol` function. We believe this bug is harmless in practice, because the out-of-bounds read accesses `malloc` metadata without causing any visible damage.This vulnerability has been patched in 0.29.0.gfm.7.	5.3	More Details
CVE-2021-4314	It is possible to manipulate the JWT token without the knowledge of the JWT secret and authenticate without valid JWT token as any user. This is happening only in the situation when zOSMF doesn’t have the APAR PH12143 applied. This issue affects: 1.16 versions to 1.19. What happens is that the services using the ZAAS client or the API ML API to query will be deceived into believing the information in the JWT token is valid when it isn’t. It’s possible to use this to persuade the southbound service that different user is authenticated.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4346	The All-In-One Security (AIOS) WordPress plugin before 5.1.3 leaked settings of the plugin publicly, including the used email address.	5.3	More Details
CVE-2023-22334	Use of password hash instead of password for authentication vulnerability in CONPROSYS HMI System (CHS) Ver.3.4.5 and earlier allows a remote authenticated attacker to obtain user credentials information via a man-in-the-middle attack.	5.3	More Details
CVE-2023-22742	libgit2 is a cross-platform, linkable library implementation of Git. When using an SSH remote with the optional libssh2 backend, libgit2 does not perform certificate checking by default. Prior versions of libgit2 require the caller to set the `certificate_check` field of libgit2's `git_remote_callbacks` structure - if a certificate check callback is not set, libgit2 does not perform any certificate checking. This means that by default - without configuring a certificate check callback, clients will not perform validation on the server SSH keys and may be subject to a man-in-the-middle attack. Users are encouraged to upgrade to v1.4.5 or v1.5.1. Users unable to upgrade should ensure that all relevant certificates are manually checked.	5.3	More Details
CVE-2022-39193	An issue was discovered in the CheckUser extension for MediaWiki through 1.39.x. Various components of this extension can expose information on the performer of edits and logged actions. This information should not allow public viewing: it is supposed to be viewable only by users with suppression rights.	5.3	More Details
CVE-2022-41733	IBM InfoSphere Information Server 11.7 could allow a remote attacked to cause some of the components to be unusable until the process is restarted. IBM X-Force ID: 237583.	5.3	More Details
CVE-2023-22912	An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. CheckUser TokenManager insecurely uses AES-CTR encryption with a repeated (aka re-used) nonce, allowing an adversary to decrypt.	5.3	More Details
CVE-2022-34399	Dell Alienware m17 R5 BIOS version prior to 1.2.2 contain a buffer access vulnerability. A malicious user with admin privileges could potentially exploit this vulnerability by sending input larger than expected in order to leak certain sections of SMRAM.	5.1	More Details
CVE-2023-21871	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2023-21863	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2023-21873	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21864	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2023-21865	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2023-21866	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2023-21887	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: GIS). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2023-21883	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2023-21867	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2023-21881	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2023-21878	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21870	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2023-21876	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2023-21879	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2023-21840	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 5.7.40 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2022-43959	Insufficiently Protected Credentials in the AD/LDAP server settings in 1C-Bitrix Bitrix24 through 22.200.200 allow remote administrators to discover an AD/LDAP administrative password by reading the source code of /bitrix/admin/ldap_server_edit.php.	4.9	More Details
CVE-2023-21836	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2023-20045	A vulnerability in the web-based management interface of Cisco Small Business RV160 and RV260 Series VPN Routers could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands using root-level privileges on the affected device. To exploit this vulnerability, the attacker must have valid Administrator-level credentials on the affected device.	4.9	More Details
CVE-2022-40697	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in 3com – Asesor de Cookies para normativa española plugin <= 3.4.3 versions.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20967	A vulnerability in the web-based management interface of Cisco Identity Services Engine could allow an authenticated, remote attacker to conduct cross-site scripting attacks against other users of the application web-based management interface. This vulnerability is due to improper validation of input to an application feature before storage within the web-based management interface. An attacker could exploit this vulnerability by creating entries within the application interface that contain malicious HTML or script code. A successful exploit could allow the attacker to store malicious HTML or script code within the application interface for use in further cross-site scripting attacks. Cisco has not yet released software updates that address this vulnerability.	4.8	More Details
CVE-2022-3811	The EU Cookie Law for GDPR/CCPA WordPress plugin through 3.1.6 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2023-20007	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code or cause the web-based management process on the device to restart unexpectedly, resulting in a denial of service (DoS) condition. The attacker must have valid administrator credentials. This vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the web-based management process to restart, resulting in a DoS condition.	4.7	More Details
CVE-2015-10067	A vulnerability was found in oznetmaster SSharpSmartThreadPool. It has been classified as problematic. This affects an unknown part of the file SSharpSmartThreadPool/SmartThreadPool.cs. The manipulation leads to race condition within a thread. The complexity of an attack is rather high. The exploitability is told to be difficult. The patch is named 0e58073c831093aad75e077962e9fb55cad0dc5f. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218463.	4.6	More Details
CVE-2023-22594	IBM Robotic Process Automation for Cloud Pak 20.12.0 through 21.0.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244075.	4.6	More Details
CVE-2023-21824	Vulnerability in the Oracle Communications BRM - Elastic Charging Engine product of Oracle Communications Applications (component: Customer, Config, Pricing Manager). Supported versions that are affected are 12.0.0.3.0-12.0.0.7.0. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Communications BRM - Elastic Charging Engine executes to compromise Oracle Communications BRM - Elastic Charging Engine. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Communications BRM - Elastic Charging Engine accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	4.4	More Details
CVE-2023-20002	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21859	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Authentication Engine). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Access Manager executes to compromise Oracle Access Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Access Manager accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	4.4	More Details
CVE-2023-21884	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details
CVE-2023-20008	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.	4.4	More Details
CVE-2023-0290	Rapid7 Velociraptor did not properly sanitize the client ID parameter to the CreateCollection API, allowing a directory traversal in where the collection task could be written. It was possible to provide a client id of "../clients/server" to schedule the collection for the server (as a server artifact), but only require privileges to schedule collections on the client. Normally, to schedule an artifact on the server, the COLLECT_SERVER permission is required. This permission is normally only granted to "administrator" role. Due to this issue, it is sufficient to have the COLLECT_CLIENT privilege, which is normally granted to the "investigator" role. To exploit this vulnerability, the attacker must already have a Velociraptor user account at least "investigator" level, and be able to authenticate to the GUI and issue an API call to the backend. Typically, most users deploy Velociraptor with limited access to a trusted group, and most users will already be administrators within the GUI. This issue affects Velociraptor versions before 0.6.7-5. Version 0.6.7-5, released January 16, 2023, fixes the issue.	4.3	More Details
CVE-2023-0406	Cross-Site Request Forgery (CSRF) in GitHub repository modoboa/modoboa prior to 2.0.4.	4.3	More Details
CVE-2022-20965	A vulnerability in the web-based management interface of Cisco Identity Services Engine could allow an authenticated, remote attacker to take privileges actions within the web-based management interface. This vulnerability is due to improper access control on a feature within the web-based management interface of the affected system. An attacker could exploit this vulnerability by accessing features through direct requests, bypassing checks within the application. A successful exploit could allow the attacker to take privileged actions within the web-based management interface that should be otherwise restricted. {{value}} ["%7b%7bvalue%7d%7d"])}]]	4.3	More Details
CVE-2022-46959	An issue in the component /admin/backups/work-dir of Sonic v1.0.4 allows attackers to execute a directory traversal.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21827	Vulnerability in the Oracle Database Data Redaction component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Oracle Database Data Redaction. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Database Data Redaction accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	4.3	More Details
CVE-2023-22630	IzyBat Orange casiers before 20221102_1 allows SQL Injection via a getCasier.php?taille= URI.	4.3	More Details
CVE-2022-46890	Weak access control in NexusPHP before 1.7.33 allows a remote authenticated user to edit any post in the forum (this is caused by a lack of checks performed by the /forums.php?action=post page).	4.3	More Details
CVE-2023-21834	Vulnerability in the Oracle Self-Service Human Resources product of Oracle E-Business Suite (component: Workflow, Approval, Work Force Management). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Self-Service Human Resources. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Self-Service Human Resources accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	4.3	More Details
CVE-2022-39429	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Easily exploitable vulnerability allows low privileged attacker having Create Procedure privilege with network access via Oracle Net to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java VM. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	4.3	More Details
CVE-2023-0385	The Custom 404 Pro plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.7.1. This is due to missing or incorrect nonce validation on the custom_404_pro_admin_init function. This makes it possible for unauthenticated attackers to delete logs, via forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-0447	The My YouTube Channel plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the clear_all_cache function in versions up to, and including, 3.0.12.1. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to clear the plugin's cache.	4.3	More Details
CVE-2021-39089	IBM Cloud Pak for Security (CP4S) 1.10.0.0 through 1.10.6.0 could allow an authenticated user to obtain sensitive information from a specially crafted HTTP request. IBM X-Force ID: 216387.	4.3	More Details
CVE-2023-24058	Booked Scheduler 2.5.5 allows authenticated users to create and schedule events for any other user via a modified userId value to reservation_save.php. NOTE: 2.5.5 is a version from 2014; the latest version of Booked Scheduler is not affected. However, LabArchives Scheduler (Sep 6, 2022 Feature Release) is affected.	4.3	More Details
CVE-2021-39011	IBM Cloud Pak for Security (CP4S) 1.10.0.0 through 1.10.6.0 stores potentially sensitive information in log files that could be read by a privileged user. IBM X-Force ID: 213645.	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22592	IBM Robotic Process Automation for Cloud Pak 21.0.1 through 21.0.4 could allow a local user to perform unauthorized actions due to insufficient permission settings. IBM X-Force ID: 244073.	4.0	More Details
CVE-2023-21900	Vulnerability in the Oracle Solaris product of Oracle Systems (component: NSSwitch). Supported versions that are affected are 10 and 11. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Solaris, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.1 Base Score 4.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:N/I:L/A:L).	4.0	More Details
CVE-2023-21885	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. Note: Applies to Windows only. CVSS 3.1 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	3.8	More Details
CVE-2023-21889	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	3.8	More Details
CVE-2023-21843	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf, 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	3.7	More Details
CVE-2023-22484	cmark-gfm is GitHub's fork of cmark, a CommonMark parsing and rendering library and program in C. Versions prior to 0.29.0.gfm.7 are subject to a polynomial time complexity issue in cmark-gfm that may lead to unbounded resource exhaustion and subsequent denial of service. This vulnerability has been patched in 0.29.0.gfm.7.	3.5	More Details
CVE-2023-22483	cmark-gfm is GitHub's fork of cmark, a CommonMark parsing and rendering library and program in C. Versions prior to 0.29.0.gfm.7 are subject to several polynomial time complexity issues in cmark-gfm that may lead to unbounded resource exhaustion and subsequent denial of service. Various commands, when piped to cmark-gfm with large values, cause the running time to increase quadratically. These vulnerabilities have been patched in version 0.29.0.gfm.7.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-25077	A vulnerability was found in melnaron mel-spintax. It has been rated as problematic. Affected by this issue is some unknown functionality of the file lib/spintax.js. The manipulation of the argument text leads to inefficient regular expression complexity. The name of the patch is 37767617846e27b87b63004e30216e8f919637d3. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-218456.	3.5	More Details
CVE-2020-36653	A vulnerability was found in GENI Portal. It has been rated as problematic. Affected by this issue is some unknown functionality of the file portal/www/portal/error-text.php. The manipulation of the argument error leads to cross site scripting. The attack may be launched remotely. The patch is identified as c2356cc41260551073bfaa3a94d1ab074f554938. It is recommended to apply a patch to fix this issue. VDB-218474 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2020-36654	A vulnerability classified as problematic has been found in GENI Portal. This affects the function no_invocation_id_error of the file portal/www/portal/sliceresource.php. The manipulation of the argument invocation_id/invocation_user leads to cross site scripting. It is possible to initiate the attack remotely. The patch is named 39a96fb4b822bd3497442a96135de498d4a81337. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218475.	3.5	More Details
CVE-2022-4892	A vulnerability was found in MyCMS. It has been classified as problematic. This affects the function build_view of the file lib/gener/view.php of the component Visitors Module. The manipulation of the argument original/converted leads to cross site scripting. It is possible to initiate the attack remotely. The patch is named d64fcba4882a50e21cdbec3eb4a080cb694d26ee. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218895.	3.5	More Details
CVE-2023-24069	Signal Desktop before 6.2.0 on Windows, Linux, and macOS allows an attacker to obtain potentially sensitive attachments sent in messages from the attachments.noindex directory. Cached attachments are not effectively cleared. In some cases, even after a self-initiated file deletion, an attacker can still recover the file if it was previously replied to in a conversation. (Local filesystem access is needed by the attacker.) NOTE: the vendor disputes the relevance of this finding because the product is not intended to protect against adversaries with this degree of local access.	3.3	More Details
CVE-2023-21882	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).	2.7	More Details
CVE-2023-21874	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Thread Pooling). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).	2.7	More Details
CVE-2022-34435	Dell iDRAC9 version 6.00.02.00 and prior contain an improper input validation vulnerability in Racadm when the firmware lock-down configuration is set. A remote high privileged attacker could exploit this vulnerability to bypass the firmware lock-down configuration and perform a firmware update.	2.7	More Details
CVE-2022-34436	Dell iDRAC8 version 2.83.83.83 and prior contain an improper input validation vulnerability in Racadm when the firmware lock-down configuration is set. A remote high privileged attacker could exploit this vulnerability to bypass the firmware lock-down configuration and perform a firmware update.	2.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2010-10006	A vulnerability, which was classified as problematic, was found in michaelliao jopenid. Affected is the function getAuthentication of the file JOpenId/src/org/expressme/openid/OpenIdManager.java. The manipulation leads to observable timing discrepancy. The complexity of an attack is rather high. The exploitability is told to be difficult. Upgrading to version 1.08 is able to address this issue. The name of the patch is c9baaa976b684637f0d5a50268e91846a7a719ab. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-218460.	2.6	More Details
CVE-2015-10071	A vulnerability was found in gitter-badger ezpublish-modern-legacy. It has been rated as problematic. This issue affects some unknown processing of the file kernel/user/forgotpassword.php. The manipulation leads to weak password recovery. The complexity of an attack is rather high. The exploitation is known to be difficult. Upgrading to version 1.0 is able to address this issue. The patch is named 5908d5ee65fec61ce0e321d586530461a210bf2a. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-218951.	2.6	More Details
CVE-2023-20057	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device.	0.0	More Details
CVE-2023-22498	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: This CVE has been rejected as it was incorrectly assigned. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2022-27918	Rejected 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 2022. Notes: none.	N/A	More Details
CVE-2022-27917	Rejected 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 2022. Notes: none.	N/A	More Details
CVE-2022-27916	Rejected 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 2022. Notes: none.	N/A	More Details
CVE-2022-27915	Rejected 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 2022. Notes: none.	N/A	More Details
CVE-2020-25714	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none.	N/A	More Details
CVE-2020-25679	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none.	N/A	More Details
CVE-2020-1715	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10765	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none.	N/A	More Details
CVE-2020-10764	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none.	N/A	More Details
CVE-2020-10694	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none.	N/A	More Details
CVE-2020-10692	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none.	N/A	More Details
CVE-2018-20104	Rejected 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 2018. Notes: none.	N/A	More Details
CVE-2022-1676	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2020-1713	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none.	N/A	More Details
CVE-2022-47016	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details