SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 20 April 2022

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-20695	A vulnerability in the authentication functionality of Cisco Wireless LAN Controller (WLC) Software could allow an unauthenticated, remote attacker to bypass authentication controls and log in to the device through the management interface This vulnerability is due to the improper implementation of the password validation algorithm. An attacker could exploit this vulnerability by logging in to an affected device with crafted credentials. A successful exploit could allow the attacker to bypass authentication and log in to the device as an administrator. The attacker could obtain privileges that are the same level as an administrative user but it depends on the crafted credentials. Note: This vulnerability exists because of a non-default device configuration that must be present for it to be exploitable. For details about the vulnerable configuration, see the Vulnerable Products section of this advisory.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24816	JAI-EXT is an open-source project which aims to extend the Java Advanced Imaging (JAI) API. Programs allowing Jiffle script to be provided via network request can lead to a Remote Code Execution as the Jiffle script is compiled into Java code via Janino, and executed. In particular, this affects the downstream GeoServer project. Version 1.2.22 will contain a patch that disables the ability to inject malicious code into the resulting script. Users unable to upgrade may negate the ability to compile Jiffle scripts from the final application, by removing janino-x.y.z.jar from the classpath.	10.0	More Details
CVE-2021-40422	An authentication bypass vulnerability exists in the device password generation functionality of Swift Sensors Gateway SG3-1010. A specially-crafted network request can lead to remote code execution. An attacker can send a sequence of requests to trigger this vulnerability.	10.0	More Details
CVE-2022-25226	ThinVNC version 1.0b1 allows an unauthenticated user to bypass the authentication process via 'http://thin-vnc:8080/cmd?cmd=connect' by obtaining a valid SID without any kind of authentication. It is possible to achieve code execution on the server by sending keyboard or mouse events to the server.	10.0	More Details
CVE-2022-21431	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Connection Manager). Supported versions that are affected are 12.0.0.4 and 12.0.0.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle Communications Billing and Revenue Management. While the vulnerability is in Oracle Communications Billing and Revenue Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Communications Billing and Revenue Management. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	10.0	More Details
CVE-2022-21420	Vulnerability in the Oracle Coherence 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 to compromise Oracle Coherence. Successful attacks of this vulnerability can result in takeover of Oracle Coherence. 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 Number	Description	Base Score	Reference
CVE-2022-27423	Chamilo LMS v1.11.13 was discovered to contain a SQL injection vulnerability via the blog_id parameter at /blog/blog.php.	9.8	More Details
CVE-2021-44486	An issue was discovered in YottaDB through r1.32 and V7.0-000. Using crafted input, attackers can manipulate the value of a function pointer used in op_write in sr_port/op_write.c in order to gain control of the flow of execution.	9.8	More Details
CVE-2021-44496	An issue was discovered in FIS GT.M through V7.0-000 (related to the YottaDB code base). Using crafted input, an attacker can control the size variable and buffer that is passed to a call to memcpy. An attacker can use this to overwrite key data structures and gain control of the flow of execution.	9.8	More Details
CVE-2022-27157	pearweb < 1.32 is suffers from a Weak Password Recovery Mechanism via include/users/passwordmanage.php.	9.8	More Details
CVE-2022-27158	pearweb < 1.32 suffers from Deserialization of Untrusted Data.	9.8	More Details
CVE-2022-24491	Windows Network File System Remote Code Execution Vulnerability	9.8	More Details
CVE-2022-24497	Windows Network File System Remote Code Execution Vulnerability	9.8	More Details
CVE-2022-26809	Remote Procedure Call Runtime Remote Code Execution Vulnerability	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21445	Vulnerability in the Oracle Application Development Framework (ADF) product of Oracle Fusion Middleware (component: ADF Faces). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Development Framework (ADF). Successful attacks of this vulnerability can result in takeover of Oracle Application Development Framework (ADF). Note: Oracle Application Development Framework (ADF) is downloaded via Oracle JDeveloper Product. Please refer to Fusion Middleware Patch Advisor for more details. 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-2022-26631	Automatic Question Paper Generator v1.0 contains a Time-Based Blind SQL injection vulnerability via the id GET parameter.	9.8	More Details
CVE-2022-0992	The SiteGround Security plugin for WordPress is vulnerable to authentication bypass that allows unauthenticated users to log in as administrative users due to missing identity verification on initial 2FA set-up that allows unauthenticated and unauthorized users to configure 2FA for pending accounts. Upon successful configuration, the attacker is logged in as that user without access to a username/password pair which is the expected first form of authentication. This affects versions up to, and including, 1.2.5.	9.8	More Details
CVE-2020-13567	Multiple SQL injection vulnerabilities exist in phpGACL 3.3.7. A specially crafted HTTP request can lead to a SQL injection. An attacker can send an HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2022-23865	Nyron 1.0 is affected by a SQL injection vulnerability through Nyron/Library/Catalog/winlibsrch.aspx. To exploit this vulnerability, an attacker must inject '"> on the thes1 parameter.	9.8	More Details
CVE-2022-0785	The Daily Prayer Time WordPress plugin before 2022.03.01 does not sanitise and escape the month parameter before using it in a SQL statement via the get_monthly_timetable AJAX action (available to unauthenticated users), leading to an unauthenticated SQL injection	9.8	More Details
CVE-2022-1020	The Product Table for WooCommerce (wooproducttable) WordPress plugin before 3.1.2 does not have authorisation and CSRF checks in the wpt_admin_update_notice_option AJAX action (available to both unauthenticated and authenticated users), as well as does not validate the callback parameter, allowing unauthenticated attackers to call arbitrary functions with either none or one user controlled argument	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29464	Certain WSO2 products allow unrestricted file upload with resultant remote code execution. The attacker must use a /fileupload endpoint with a Content-Disposition directory traversal sequence to reach a directory under the web root, such as a ../../../../repository/deployment/server/webapps directory. This affects WSO2 API Manager 2.2.0 up to 4.0.0, WSO2 Identity Server 5.2.0 up to 5.11.0, WSO2 Identity Server Analytics 5.4.0, 5.4.1, 5.5.0 and 5.6.0, WSO2 Identity Server as Key Manager 5.3.0 up to 5.11.0, WSO2 Enterprise Integrator 6.2.0 up to 6.6.0, WSO2 Open Banking AM 1.4.0 up to 2.0.0 and WSO2 Open Banking KM 1.4.0, up to 2.0.0.	9.8	More Details
CVE-2022-27927	A SQL injection vulnerability exists in Microfinance Management System 1.0 when MySQL is being used as the application database. An attacker can issue SQL commands to the MySQL database through the vulnerable course_code and/or customer_number parameter.	9.8	More Details
CVE-2022-27104	An Unauthenticated time-based blind SQL injection vulnerability exists in Forma LMS prior to v.1.4.3.	9.8	More Details
CVE-2021-42230	Seowon 130-SLC router all versions as of 2021-09-15 is vulnerable to Remote Code Execution via the queriesCnt parameter.	9.8	More Details
CVE-2021-43741	CMSimple 5.4 is vulnerable to Directory Traversal. The vulnerability exists when a user changes the file name to malicious file on config.php leading to remote code execution.	9.8	More Details
CVE-2022-27007	nginx njs 0.7.2 is affected suffers from Use-after-free in njs_function_frame_alloc() when it try to invoke from a restored frame saved with njs_function_frame_save().	9.8	More Details
CVE-2021-40390	An authentication bypass vulnerability exists in the Web Application functionality of Moxa MXView Series 3.2.4. A specially-crafted HTTP request can lead to unauthorized access. An attacker can send an HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2022-22955	VMware Workspace ONE Access has two authentication bypass vulnerabilities (CVE-2022-22955 & CVE-2022-22956) in the OAuth2 ACS framework. A malicious actor may bypass the authentication mechanism and execute any operation due to exposed endpoints in the authentication framework.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22956	VMware Workspace ONE Access has two authentication bypass vulnerabilities (CVE-2022-22955 & CVE-2022-22956) in the OAuth2 ACS framework. A malicious actor may bypass the authentication mechanism and execute any operation due to exposed endpoints in the authentication framework.	9.8	More Details
CVE-2022-27479	Apache Superset before 1.4.2 is vulnerable to SQL injection in chart data requests. Users should update to 1.4.2 or higher which addresses this issue.	9.8	More Details
CVE-2021-43290	An issue was discovered in ThoughtWorks GoCD before 21.3.0. An attacker who has compromised a GoCD agent can upload a malicious file into a directory of a GoCD server. They can control the filename but the directory is placed inside of a directory that they can't control.	9.8	More Details
CVE-2022-26507	A heap-based buffer overflow exists in XML Decompression DecodeTreeBlock in AT&T Labs Xmill 0.7. A crafted input file can lead to remote code execution. This is not the same as any of: CVE-2021-21810, CVE-2021-21811, CVE-2021-21812, CVE-2021-21815, CVE-2021-21825, CVE-2021-21826, CVE-2021-21828, CVE-2021-21829, or CVE-2021-21830. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	9.8	More Details
CVE-2022-28044	lrzip v0.640 was discovered to contain a heap memory corruption via the component lrzip.c:initialise_control.	9.8	More Details
CVE-2021-21938	A heap-based buffer overflow vulnerability exists in the Palette box parser functionality of Accusoft ImageGear 19.10. A specially-crafted file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2022-27862	Arbitrary File Upload leading to RCE in E4J s.r.l. VikBooking Hotel Booking Engine & PMS plugin <= 1.5.3 on WordPress allows attackers to upload and execute dangerous file types (e.g. PHP shell) via the signature upload on the booking form.	9.8	More Details
CVE-2022-28711	A memory corruption vulnerability exists in the cgi.c unescape functionality of ArduPilot APWeb master branch 50b6b7ac - master branch 46177cb9. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability.	9.8	More Details
CVE-2021-40386	Kaseya Unitrends Client/Agent through 10.5,5 allows remote attackers to execute arbitrary code.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26651	An issue was discovered in Asterisk through 19.x and Certified Asterisk through 16.8-cert13. The func_odbc module provides possibly inadequate escaping functionality for backslash characters in SQL queries, resulting in user-provided data creating a broken SQL query or possibly a SQL injection. This is fixed in 16.25.2, 18.11.2, and 19.3.2, and 16.8-cert14.	9.8	More Details
CVE-2022-24846	GeoWebCache is a tile caching server implemented in Java. The GeoWebCache disk quota mechanism can perform an unchecked JNDI lookup, which in turn can be used to perform class deserialization and result in arbitrary code execution. While in GeoWebCache the JNDI strings are provided via local configuration file, in GeoServer a user interface is provided to perform the same, that can be accessed remotely, and requires admin-level login to be used. These lookup are unrestricted in scope and can lead to code execution. The lookups are going to be restricted in GeoWebCache 1.21.0, 1.20.2, 1.19.3.	9.1	More Details
CVE-2022-26034	Improper authentication vulnerability in the communication protocol provided by AD (Automation Design) server of CENTUM VP R6.01.10 to R6.09.00, CENTUM VP Small R6.01.10 to R6.09.00, CENTUM VP Basic R6.01.10 to R6.09.00, and B/M9000 VP R8.01.01 to R8.03.01 allows an attacker to use the functions provided by AD server. This may lead to leakage or tampering of data managed by AD server.	9.1	More Details
CVE-2022-26499	An SSRF issue was discovered in Asterisk through 19.x. When using STIR/SHAKEN, it's possible to send arbitrary requests (such as GET) to interfaces such as localhost by using the Identity header. This is fixed in 16.25.2, 18.11.2, and 19.3.2.	9.1	More Details
CVE-2021-44488	An issue was discovered in YottaDB through r1.32 and V7.0-000. Using crafted input, attackers can control the size and input to calls to memcpy in op_fnfnumber in sr_port/op_fnfnumber.c in order to corrupt memory or crash the application.	9.1	More Details
CVE-2021-22795	A CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability exists that could cause remote code execution when performed over the network. Affected Product: StruxureWare Data Center Expert (V7.8.1 and prior)	9.1	More Details
CVE-2021-22794	A CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could cause remote code execution. Affected Product: StruxureWare Data Center Expert (V7.8.1 and prior)	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1345	Stored XSS viva .svg file upload in GitHub repository causefx/organizr prior to 2.1.1810. This allows attackers to execute malicious scripts in the user's browser and it can lead to session hijacking, sensitive data exposure, and worse.	9.0	More Details
CVE-2022-1346	Multiple Stored XSS in GitHub repository causefx/organizr prior to 2.1.1810. This allows attackers to execute malicious scripts in the user's browser and it can lead to session hijacking, sensitive data exposure, and worse.	9.0	More Details
CVE-2022-1344	Stored XSS due to no sanitization in the filename in GitHub repository causefx/organizr prior to 2.1.1810. This allows attackers to execute malicious scripts in the user's browser and it can lead to session hijacking, sensitive data exposure, and worse.	9.0	More Details
CVE-2021-42136	A stored Cross-Site Scripting (XSS) vulnerability in the Missing Data Codes functionality of REDCap before 11.4.0 allows remote attackers to execute JavaScript code in the client's browser by storing said code as a Missing Data Code value. This can then be leveraged to execute a Cross-Site Request Forgery attack to escalate privileges to administrator.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-44520	In Citrix XenMobile Server through 10.12 RP9, there is an Authenticated Command Injection vulnerability, leading to remote code execution with root privileges.	8.8	More Details
CVE-2020-28635	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_sedge() seh->facet().	8.8	More Details
CVE-2020-35632	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_sface() sfh->boundary_entry_objects Edge_of.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28042	stb_image.h v2.27 was discovered to contain an heap-based use-after-free via the function stbi__jpeg_huff_decode.	8.8	More Details
CVE-2022-28048	STB v2.27 was discovered to contain an integer shift of invalid size in the component stbi__jpeg_decode_block_prog_ac.	8.8	More Details
CVE-2020-35631	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_sface() SD.link_as_face_cycle().	8.8	More Details
CVE-2020-35630	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_sface() sfh->center_vertex().	8.8	More Details
CVE-2020-35629	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_sloop() slh->facet().	8.8	More Details
CVE-2020-28634	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_sedge() seh->next().	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28625	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_facet() fh->boundary_entry_objects SLoop_of.	8.8	More Details
CVE-2020-28633	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_sedge() seh->prev().	8.8	More Details
CVE-2020-28632	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_sedge() seh->incident_sface().	8.8	More Details
CVE-2020-28631	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_sedge() seh->source().	8.8	More Details
CVE-2020-28629	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_sedge() seh->sprev().	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28628	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_volume() seh->twin().	8.8	More Details
CVE-2020-28627	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_volume() ch->shell_entry_objects().	8.8	More Details
CVE-2022-29457	Zoho ManageEngine ADSelfService Plus before 6121, ADAuditPlus 7060, Exchange Reporter Plus 5701, and ADManagerPlus 7131 allow NTLM Hash disclosure during certain storage-path configuration steps.	8.8	More Details
CVE-2022-22149	A SQL injection vulnerability exists in the HelpdeskEmailActions.aspx functionality of Lansweeper lansweeper 9.1.20.2. A specially-crafted HTTP request can cause SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2022-21234	An SQL injection vulnerability exists in the EchoAssets.aspx functionality of Lansweeper lansweeper 9.1.20.2. A specially-crafted HTTP request can cause SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2022-21210	An SQL injection vulnerability exists in the AssetActions.aspx functionality of Lansweeper lansweeper 9.1.20.2. A specially-crafted HTTP request can cause SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2021-40426	A heap-based buffer overflow vulnerability exists in the sphere.c start_read() functionality of Sound Exchange libsox 14.4.2 and master commit 42b3557e. A specially-crafted file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger this vulnerability.	8.8	More Details
CVE-2022-28108	Selenium Server (Grid) before 4 allows CSRF because it permits non-JSON content types such as application/x-www-form-urlencoded, multipart/form-data, and text/plain.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21949	An improper array index validation vulnerability exists in the JPEG-JFIF Scan header parser functionality of Accusoft ImageGear 19.10. A specially-crafted file can lead to an out-of-bounds write and potential code exectuion. An attacker can provide a malicious file to trigger this vulnerability.	8.8	More Details
CVE-2021-21947	Two heap-based buffer overflow vulnerabilities exists in the JPEG-JFIF lossless Huffman image parser functionality of Accusoft ImageGear 19.10. A specially-crafted file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger these vulnerabilities.This heap-based buffer overflow takes place when the `SOF3` precision is greater or equal than 9.	8.8	More Details
CVE-2021-21946	Two heap-based buffer overflow vulnerabilities exists in the JPEG-JFIF lossless Huffman image parser functionality of Accusoft ImageGear 19.10. A specially-crafted file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger these vulnerabilities.This heap-based buffer overflow takes place when the `SOF3` precision is lower than 9.	8.8	More Details
CVE-2021-21945	Two heap-based buffer overflow vulnerabilities exist in the TIFF parser functionality of Accusoft ImageGear 19.10. A specially-crafted file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger these vulnerabilities.This heap-based buffer oveflow takes place trying to copy the second 12 bits from local variable.	8.8	More Details
CVE-2021-21944	Two heap-based buffer overflow vulnerabilities exist in the TIFF parser functionality of Accusoft ImageGear 19.10. A specially-crafted file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger these vulnerabilities.This heap-based buffer oveflow takes place trying to copy the first 12 bits from local variable.	8.8	More Details
CVE-2021-21943	A heap-based buffer overflow vulnerability exists in the XWD parser functionality of Accusoft ImageGear 19.10. A specially-crafted file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	8.8	More Details
CVE-2021-21942	An out-of-bounds write vulnerability exists in the TIFF YCbCr image parser functionality of Accusoft ImageGear 19.10. A specially-crafted file can lead to remote code execution. An attacker can provide a malicious file to trigger this vulnerability.	8.8	More Details
CVE-2021-21939	A heap-based buffer overflow vulnerability exists in the XWD parser functionality of Accusoft ImageGear 19.10. A specially-crafted file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21914	A heap-based buffer overflow vulnerability exists in the DecoderStream::Append functionality of Accusoft ImageGear 19.10. A specially-crafted file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	8.8	More Details
CVE-2022-29315	Invicti Acunetix before 14 allows CSV injection via the Description field on the Add Targets page, if the Export CSV feature is used.	8.8	More Details
CVE-2021-44519	In Citrix XenMobile Server through 10.12 RP9, there is an Authenticated Directory Traversal vulnerability, leading to remote code execution.	8.8	More Details
CVE-2020-28626	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_facet() fh->incident_volume().	8.8	More Details
CVE-2020-28624	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_facet() fh->boundary_entry_objects SEdge_of.	8.8	More Details
CVE-2021-26625	Insufficient Verification of input Data leading to arbitrary file download and execute was discovered in Nexacro platform. This vulnerability is caused by an automatic update function that does not verify input data except version information. Remote attackers can use this incomplete validation logic to download and execute arbitrary malicious file.	8.8	More Details
CVE-2022-24500	Windows SMB Remote Code Execution Vulnerability	8.8	More Details
CVE-2020-28608	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_2/PM_io_parser.h PM_io_parser<PMDEC>::read_face() store_fc().	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28607	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_2/PM_io_parser.h PM_io_parser<PMDEC>::read_face() set_halfedge().	8.8	More Details
CVE-2022-24487	Windows Local Security Authority Subsystem Service (LSASS) Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-24492	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2020-28606	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_2/PM_io_parser.h PM_io_parser<PMDEC>::read_hedge() e->set_face().	8.8	More Details
CVE-2020-28605	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read exists in Nef_2/PM_io_parser.h PM_io_parser<PMDEC>::read_hedge() e->set_vertex().	8.8	More Details
CVE-2022-24528	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2020-28623	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_facet() fh->twin().	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28604	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_2/PM_io_parser.h PM_io_parser<PMDEC>::read_hedge() e->set_next().	8.8	More Details
CVE-2022-24541	Windows Server Service Remote Code Execution Vulnerability	8.8	More Details
CVE-2020-28603	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_2/PM_io_parser.h PM_io_parser<PMDEC>::read_hedge() e->set_prev().	8.8	More Details
CVE-2020-28602	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_2/PM_io_parser.h PM_io_parser<PMDEC>::read_vertex() Halfedge_of[].	8.8	More Details
CVE-2022-27908	Zoho ManageEngine OpManager before 125588 (and before 125603) is vulnerable to authenticated SQL Injection in the Inventory Reports module.	8.8	More Details
CVE-2022-29281	Notable before 1.9.0-beta.8 doesn't effectively prevent the opening of executable files when clicking on a link. There is improper validation of the file URI scheme. A hyperlink to an SMB share could lead to execution of an arbitrary program (or theft of NTLM credentials via an SMB relay attack, because the application resolves UNC paths).	8.8	More Details
CVE-2020-28609	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_2/PM_io_parser.h PM_io_parser<PMDEC>::read_face() store_iv().	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28610	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SM_io_parser.h SM_io_parser<Decorator_>::read_vertex() set_face().	8.8	More Details
CVE-2022-23259	Microsoft Dynamics 365 On-Premises Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-23257	Windows Hyper-V Remote Code Execution Vulnerability	8.8	More Details
CVE-2020-28611	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SM_io_parser.h SM_io_parser<Decorator_>::read_vertex() set_first_out_edge().	8.8	More Details
CVE-2020-28612	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_vertex() vh->svertices_begin().	8.8	More Details
CVE-2020-28613	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_vertex() vh->svertices_last().	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28614	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_vertex() vh->shalfedges_begin().	8.8	More Details
CVE-2020-28615	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_vertex() vh->shalfedges_last().	8.8	More Details
CVE-2020-28616	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_vertex() vh->sfaces_begin().	8.8	More Details
CVE-2022-28109	Selenium Selenium Grid (formerly Selenium Standalone Server) Fixed in 4.0.0-alpha-7 is affected by: DNS rebinding. The impact is: execute arbitrary code (remote). The component is: WebDriver endpoint of Selenium Grid / Selenium Standalone Server. The attack vector is: Triggered by browsing to to a malicious remote web server. The WebDriver endpoint of Selenium Server (Grid) is vulnerable to DNS rebinding. This can be used to execute arbitrary code on the machine.	8.8	More Details
CVE-2020-28617	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_vertex() vh->sfaces_last().	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28618	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_vertex() vh->shalfloop().	8.8	More Details
CVE-2020-28619	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_edge() eh->twin().	8.8	More Details
CVE-2020-28620	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_edge() eh->center_vertex():.	8.8	More Details
CVE-2020-28621	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_edge() eh->out_sedge().	8.8	More Details
CVE-2020-28622	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_edge() eh->incident_sface().	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22182	A Cross-site Scripting (XSS) vulnerability in Juniper Networks Junos OS J-Web allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. This issue affects: Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S19; 15.1 versions prior to 15.1R7-S10; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S10, 18.4R3-S9; 19.1 versions prior to 19.1R2-S3, 19.1R3-S6; 19.2 versions prior to 19.2R1-S8, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2; 21.2 versions prior to 21.2R1-S1, 21.2R2.	8.8	More Details
CVE-2020-28630	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger any of these vulnerabilities. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_sedge() seh->snext().	8.8	More Details
CVE-2022-27426	A Server-Side Request Forgery (SSRF) in Chamilo LMS v1.11.13 allows attackers to enumerate the internal network and execute arbitrary system commands via a crafted Phar file.	8.8	More Details
CVE-2021-4096	The Fancy Product Designer plugin for WordPress is vulnerable to Cross-Site Request Forgery via the FPD_Admin_Import class that makes it possible for attackers to upload malicious files that could be used to gain webshell access to a server in versions up to, and including, 4.7.5.	8.8	More Details
CVE-2021-3100	The Apache Log4j hotpatch package before log4j-cve-2021-44228-hotpatch-1.1-13 didn’t mimic the permissions of the JVM being patched, allowing it to escalate privileges.	8.8	More Details
CVE-2021-3101	Hotdog, prior to v1.0.1, did not mimic the capabilities or the SELinux label of the target JVM process. This would allow a container to gain full privileges on the host, bypassing restrictions set on the container.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21442	Vulnerability in Oracle GoldenGate (component: OGG Core Library). The supported version that is affected is Prior to 23.1. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle GoldenGate executes to compromise Oracle GoldenGate. While the vulnerability is in Oracle GoldenGate, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle GoldenGate. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	8.8	More Details
CVE-2022-24845	Vyper is a pythonic Smart Contract Language for the ethereum virtual machine. In affected versions, the return of `<iface>.returns_int128()` is not validated to fall within the bounds of `int128`. This issue can result in a misinterpretation of the integer value and lead to incorrect behavior. As of v0.3.0, `<iface>.returns_int128()` is validated in simple expressions, but not complex expressions. Users are advised to upgrade. There is no known workaround for this issue.	8.8	More Details
CVE-2022-0070	Incomplete fix for CVE-2021-3100. The Apache Log4j hotpatch package starting with log4j-cve-2021-44228-hotpatch-1.1-16 will now explicitly mimic the Linux capabilities and cgroups of the target Java process that the hotpatch is applied to.	8.8	More Details
CVE-2022-1329	The Elementor Website Builder plugin for WordPress is vulnerable to unauthorized execution of several AJAX actions due to a missing capability check in the ~/core/app/modules/onboarding/module.php file that make it possible for attackers to modify site data in addition to uploading malicious files that can be used to obtain remote code execution, in versions 3.6.0 to 3.6.2.	8.8	More Details
CVE-2021-43286	An issue was discovered in ThoughtWorks GoCD before 21.3.0. An attacker with privileges to create a new pipeline on a GoCD server can abuse a command-line injection in the Git URL "Test Connection" feature to execute arbitrary code.	8.8	More Details
CVE-2022-0071	Incomplete fix for CVE-2021-3101. Hotdog, prior to v1.0.2, did not mimic the resource limits, device restrictions, or syscall filters of the target JVM process. This would allow a container to exhaust the resources of the host, modify devices, or make syscalls that would otherwise be blocked.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24855	Metabase is an open source business intelligence and analytics application. In affected versions Metabase ships with an internal development endpoint `/_internal` that can allow for cross site scripting (XSS) attacks, potentially leading to phishing attempts with malicious links that could lead to account takeover. Users are advised to either upgrade immediately, or block access in your firewall to `/_internal` endpoints for Metabase. The following patches (or greater versions) are available: 0.42.4 and 1.42.4, 0.41.7 and 1.41.7, 0.40.8 and 1.40.8.	8.7	More Details
CVE-2022-20622	A vulnerability in IP ingress packet processing of the Cisco Embedded Wireless Controller with Catalyst Access Points Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, causing a denial of service (DoS) condition. The device may experience a performance degradation in traffic processing or high CPU usage prior to the unexpected reload. This vulnerability is due to improper rate limiting of IP packets to the management interface. An attacker could exploit this vulnerability by sending a steady stream of IP traffic at a high rate to the management interface of the affected device. A successful exploit could allow the attacker to cause the device to reload.	8.6	More Details
CVE-2022-20678	A vulnerability in the AppNav-XE feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of certain TCP segments. An attacker could exploit this vulnerability by sending a stream of crafted TCP traffic at a high rate through an interface of an affected device. That interface would need to have AppNav interception enabled. A successful exploit could allow the attacker to cause the device to reload.	8.6	More Details
CVE-2022-20682	A vulnerability in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol processing of Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Family could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to inadequate input validation of incoming CAPWAP packets encapsulating multicast DNS (mDNS) queries. An attacker could exploit this vulnerability by connecting to a wireless network and sending a crafted mDNS query, which would flow through and be processed by the wireless controller. A successful exploit could allow the attacker to cause the affected device to crash and reload, resulting in a DoS condition.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20683	A vulnerability in the Application Visibility and Control (AVC-FNF) feature of Cisco IOS XE Software for Cisco Catalyst 9800 Series Wireless Controllers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient packet verification for traffic inspected by the AVC feature. An attacker could exploit this vulnerability by sending crafted packets from the wired network to a wireless client, resulting in the crafted packets being processed by the wireless controller. A successful exploit could allow the attacker to cause a crash and reload of the affected device, resulting in a DoS condition.	8.6	More Details
CVE-2022-20697	A vulnerability in the web services interface of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. This vulnerability is due to improper resource management in the HTTP server code. An attacker could exploit this vulnerability by sending a large number of HTTP requests to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	8.6	More Details
CVE-2022-20714	A vulnerability in the data plane microcode of Lightspeed-Plus line cards for Cisco ASR 9000 Series Aggregation Services Routers could allow an unauthenticated, remote attacker to cause the line card to reset. This vulnerability is due to the incorrect handling of malformed packets that are received on the Lightspeed-Plus line cards. An attacker could exploit this vulnerability by sending a crafted IPv4 or IPv6 packet through an affected device. A successful exploit could allow the attacker to cause the Lightspeed-Plus line card to reset, resulting in a denial of service (DoS) condition for any traffic that traverses that line card.	8.6	More Details
CVE-2022-21430	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Connection Manager). Supported versions that are affected are 12.0.0.4 and 12.0.0.5. Difficult to exploit vulnerability allows low privileged attacker with network access via TCP to compromise Oracle Communications Billing and Revenue Management. While the vulnerability is in Oracle Communications Billing and Revenue Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Communications Billing and Revenue Management. CVSS 3.1 Base Score 8.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	8.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1347	Stored XSS in the "Username" & "Email" input fields leads to account takeover of Admin & Co-admin users in GitHub repository causefx/organizr prior to 2.1.1810. Account takeover and privilege escalation	8.4	More Details
CVE-2022-1258	A blind SQL injection vulnerability in the ePolicy Orchestrator (ePO) extension of MA prior to 5.7.6 can be exploited by an authenticated administrator on ePO to perform arbitrary SQL queries in the back-end database, potentially leading to command execution on the server.	8.4	More Details
CVE-2022-24828	Composer is a dependency manager for the PHP programming language. Integrators using Composer code to call `VcsDriver::getFileContent` can have a code injection vulnerability if the user can control the `$file` or `$identifier` argument. This leads to a vulnerability on packagist.org for example where the composer.json's `readme` field can be used as a vector for injecting parameters into hg/Mercurial via the `$file` argument, or git via the `$identifier` argument if you allow arbitrary data there (Packagist does not, but maybe other integrators do). Composer itself should not be affected by the vulnerability as it does not call `getFileContent` with arbitrary data into `$file`/`$identifier`. To the best of our knowledge this was not abused, and the vulnerability has been patched on packagist.org and Private Packagist within a day of the vulnerability report.	8.3	More Details
CVE-2022-21424	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Connection Manager). The supported version that is affected is 12.0.0.4. Easily exploitable vulnerability allows low privileged attacker with network access via TCP to compromise Oracle Communications Billing and Revenue Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Communications Billing and Revenue Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Communications Billing and Revenue Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Communications Billing and Revenue Management. CVSS 3.1 Base Score 8.3 (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:L).	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21446	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Utility). The supported version that is affected is 11. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Solaris accessible data as well as unauthorized read access to a subset of Oracle Solaris accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N).	8.2	More Details
CVE-2022-24818	GeoTools is an open source Java library that provides tools for geospatial data. The GeoTools library has a number of data sources that can perform unchecked JNDI lookups, which in turn can be used to perform class deserialization and result in arbitrary code execution. Similar to the Log4J case, the vulnerability can be triggered if the JNDI names are user-provided, but requires admin-level login to be triggered. The lookups are now restricted in GeoTools 26.4, GeoTools 25.6, and GeoTools 24.6. Users unable to upgrade should ensure that any downstream application should not allow usage of remotely provided JNDI strings.	8.2	More Details
CVE-2022-21464	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Business Logic Infra SEC). The supported version that is affected is Prior to 9.2.6.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of JD Edwards EnterpriseOne Tools and unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H).	8.2	More Details
CVE-2022-24545	Windows Kerberos Remote Code Execution Vulnerability	8.1	More Details
CVE-2022-26919	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	8.1	More Details
CVE-2022-23976	Cross-Site Request Forgery (CSRF) in Access Demo Importer <= 1.0.7 on WordPress allows an attacker to reset all data (posts / pages / media).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24851	LDAP Account Manager (LAM) is an open source web frontend for managing entries stored in an LDAP directory. The profile editor tool has an edit profile functionality, the parameters on this page are not properly sanitized and hence leads to stored XSS attacks. An authenticated user can store XSS payloads in the profiles, which gets triggered when any other user try to access the edit profile page. The pdf editor tool has an edit pdf profile functionality, the logoFile parameter in it is not properly sanitized and an user can enter relative paths like ../../../../../../../../../../../usr/share/icons/hicolor/48x48/apps/gvim.png via tools like burpsuite. Later when a pdf is exported using the edited profile the pdf icon has the image on that path(if image is present). Both issues require an attacker to be able to login to LAM admin interface. The issue is fixed in version 7.9.1.	8.1	More Details
CVE-2022-21404	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Reactive WebServer). Supported versions that are affected are 1.4.10 and 2.0.0-RC1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in takeover of Helidon. 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-2022-1065	A vulnerability within the authentication process of Abacus ERP allows a remote attacker to bypass the second authentication factor. This issue affects: Abacus ERP v2022 versions prior to R1 of 2022-01-15; v2021 versions prior to R4 of 2022-01-15; v2020 versions prior to R6 of 2022-01-15; v2019 versions later than R5 (service pack); v2018 versions later than R5 (service pack). This issue does not affect: Abacus ERP v2019 versions prior to R5 of 2020-03-15; v2018 versions prior to R7 of 2020-04-15; v2017 version and prior versions and prior versions.	8.1	More Details
CVE-2022-24539	Windows Hyper-V Shared Virtual Hard Disks Information Disclosure Vulnerability	8.1	More Details
CVE-2022-24844	Gin-vue-admin is a backstage management system based on vue and gin, which separates the front and rear of the full stack. The problem occurs in the following code in server/service/system/sys_auto_code_pgsql.go, which means that PostgreSQL must be used as the database for this vulnerability to occur. Users must: Require JWT login） and be using PostgreSQL to be affected. This issue has been resolved in version 2.5.1. There are no known workarounds.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21497	Vulnerability in the Oracle Web Services Manager product of Oracle Fusion Middleware (component: Web Services Security). Supported versions that are affected are 12.2.1.3.0 and 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-2022-24490	Windows Hyper-V Shared Virtual Hard Disks Information Disclosure Vulnerability	8.1	More Details
CVE-2021-36205	Under certain circumstances the session token is not cleared on logout.	8.1	More Details
CVE-2022-0993	The SiteGround Security plugin for WordPress is vulnerable to authentication bypass that allows unauthenticated users to log in as administrative users due to missing identity verification on the 2FA back-up code implementation that logs users in upon success. This affects versions up to, and including, 1.2.5.	8.1	More Details
CVE-2021-26626	Improper input validation vulnerability in XPLATFORM's execBrowser method can cause execute arbitrary commands. IF the second parameter value of the execBrowser function is ‘default’, the first parameter value could be passed to the ShellExecuteW API. The passed parameter is an arbitrary code to be executed. Remote attackers can use this vulnerability to execute arbitrary remote code.	8.1	More Details
CVE-2022-25648	The package git before 1.11.0 are vulnerable to Command Injection via git argument injection. When calling the fetch(remote = 'origin', opts = {}) function, the remote parameter is passed to the git fetch subcommand in a way that additional flags can be set. The additional flags can be used to perform a command injection.	8.1	More Details
CVE-2022-24472	Microsoft SharePoint Server Spoofing Vulnerability	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22181	A reflected Cross-site Scripting (XSS) vulnerability in J-Web of Juniper Networks Junos OS allows a network-based authenticated attacker to run malicious scripts reflected off J-Web to the victim's browser in the context of their session within J-Web. This may allow the attacker to gain control of the device or attack other authenticated user sessions. This issue affects: Juniper Networks Junos OS All versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2.	8.0	More Details
CVE-2022-24533	Remote Desktop Protocol Remote Code Execution Vulnerability	8.0	More Details
CVE-2022-24854	Metabase is an open source business intelligence and analytics application. SQLite has an FDW-like feature called `ATTACH DATABASE`, which allows connecting multiple SQLite databases via the initial connection. If the attacker has SQL permissions to at least one SQLite database, then it can attach this database to a second database, and then it can query across all the tables. To be able to do that the attacker also needs to know the file path to the second database. Users are advised to upgrade as soon as possible. If you're unable to upgrade, you can modify your SQLIte connection strings to contain the url argument `?limit_attached=0`, which will disallow making connections to other SQLite databases. Only users making use of SQLite are affected.	8.0	More Details
CVE-2022-28052	Directory Traversal vulnerability in file cn/roothub/store/FileSystemStorageService in function store in Roothub 2.6.0 allows remote attackers with low privlege to arbitrarily upload files via /common/upload API, which could lead to remote arbitrary code execution.	8.0	More Details
CVE-2022-24532	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-20716	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain escalated privileges. This vulnerability is due to improper access control on files within the affected system. A local attacker could exploit this vulnerability by modifying certain files on the vulnerable device. If successful, the attacker could gain escalated privileges and take actions on the system with the privileges of the root user.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24537	Windows Hyper-V Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-22009	Windows Hyper-V Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-22187	An Improper Privilege Management vulnerability in the Windows Installer framework used in the Juniper Networks Juniper Identity Management Service (JIMS) allows an unprivileged user to trigger a repair operation. Running a repair operation, in turn, will trigger a number of file operations in the %TEMP% folder of the user triggering the repair. Some of these operations will be performed from a SYSTEM context (started via the Windows Installer service), including the execution of temporary files. An attacker may be able to provide malicious binaries to the Windows Installer, which will be executed with high privilege, leading to a local privilege escalation. This issue affects Juniper Networks Juniper Identity Management Service (JIMS) versions prior to 1.4.0.	7.8	More Details
CVE-2022-24542	Windows Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-24543	Windows Upgrade Assistant Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-20681	A vulnerability in the CLI of Cisco IOS XE Software for Cisco Catalyst 9000 Family Switches and Cisco Catalyst 9000 Family Wireless Controllers could allow an authenticated, local attacker to elevate privileges to level 15 on an affected device. This vulnerability is due to insufficient validation of user privileges after the user executes certain CLI commands. An attacker could exploit this vulnerability by logging in to an affected device as a low-privileged user and then executing certain CLI commands. A successful exploit could allow the attacker to execute arbitrary commands with level 15 privileges on the affected device.	7.8	More Details
CVE-2022-22008	Windows Hyper-V Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-24544	Windows Kerberos Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29072	7-Zip through 21.07 on Windows allows privilege escalation and command execution when a file with the .7z extension is dragged to the Help>Contents area. This is caused by misconfiguration of 7z.dll and a heap overflow. The command runs in a child process under the 7zFM.exe process. NOTE: multiple third parties have reported that no privilege escalation can occur	7.8	More Details
CVE-2022-24546	Windows DWM Core Library Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-40398	An out-of-bounds write vulnerability exists in the parse_raster_data functionality of Accusoft ImageGear 19.10. A specially-crafted malformed file can lead to memory corruption. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2022-24549	Windows AppX Package Manager Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-24550	Windows Telephony Server Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-29156	drivers/infiniband/ulp/rtrs/rtrs-clt.c in the Linux kernel before 5.16.12 has a double free related to rtrs_clt_dev_release.	7.8	More Details
CVE-2022-26786	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-26787	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-24530	Windows Installer Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-24547	Windows Digital Media Receiver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-27527	A Memory Corruption vulnerability may lead to code execution through maliciously crafted DLL files. It was fixed in PDFTron earlier than 9.0.7 version in Autodesk Navisworks 2022, and 2020.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25795	A Memory Corruption Vulnerability in Autodesk TrueView 2022 and 2021 may lead to remote code execution through maliciously crafted DWG files.	7.8	More Details
CVE-2022-24474	Windows Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-24479	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-24481	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-22960	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a privilege escalation vulnerability due to improper permissions in support scripts. A malicious actor with local access can escalate privileges to 'root'.	7.8	More Details
CVE-2021-22797	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal) vulnerability exists that could cause malicious script to be deployed in an unauthorized location and may result in code execution on the engineering workstation when a malicious project file is loaded in the engineering software. Affected Product: EcoStruxure Control Expert (V15.0 SP1 and prior, including former Unity Pro), EcoStruxure Process Expert (2020 and prior, including former HDCS), SCADAPack RemoteConnect for x70 (All versions)	7.8	More Details
CVE-2022-24486	Windows Kerberos Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-46167	An access control issue in the authentication module of wizplat PD065 v1.19 allows attackers to access sensitive data and cause a Denial of Service (DoS).	7.8	More Details
CVE-2022-24488	Windows Desktop Bridge Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-24489	Cluster Client Failover (CCF) Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3624	There is an integer overflow vulnerability in dcraw. When the victim runs dcraw with a maliciously crafted X3F input image, arbitrary code may be executed in the victim's system.	7.8	More Details
CVE-2022-25797	A maliciously crafted PDF file in Autodesk AutoCAD 2022, 2021, 2020, 2019 can be used to dereference for a write beyond the allocated buffer while parsing PDF files. The vulnerability exists because the application fails to handle a crafted PDF file, which causes an unhandled exception.	7.8	More Details
CVE-2022-21491	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.34. 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 takeover of Oracle VM VirtualBox. Note: This vulnerability applies to Windows systems only. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	7.8	More Details
CVE-2022-24494	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-24496	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-24499	Windows Installer Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-25788	A maliciously crafted JT file in Autodesk AutoCAD 2022 may be used to write beyond the allocated buffer while parsing JT files. This vulnerability can be exploited to execute arbitrary code.	7.8	More Details
CVE-2022-24513	Visual Studio Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-24521	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-24527	Microsoft Endpoint Configuration Manager Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6099	An exploitable code execution vulnerability exists in the file format parsing functionality of Graphisoft BIMx Desktop Viewer 2019.2.2328. A specially crafted file can cause a heap buffer overflow resulting in a code execution. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2022-26788	PowerShell Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-21154	An integer overflow vulnerability exists in the fltSaveCMP functionality of Leadtools 22. A specially-crafted BMP file can lead to an integer overflow, that in turn causes a buffer overflow. An attacker can provide a malicious BMP file to trigger this vulnerability.	7.8	More Details
CVE-2022-26802	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-26789	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-26803	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-26810	Windows File Server Resource Management Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-21948	A heap-based buffer overflow vulnerability exists in the readDatHeadVec functionality of AnyCubic Chitubox AnyCubic Plugin 1.0.0. A specially-crafted GF file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2022-1256	A local privilege escalation vulnerability in MA for Windows prior to 5.7.6 allows a local low privileged user to gain system privileges through running the repair functionality. Temporary file actions were performed on the local user's %TEMP% directory with System privileges through manipulation of symbolic links.	7.8	More Details
CVE-2022-26901	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26903	Windows Graphics Component Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-26798	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-26914	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-26916	Windows Fax Compose Form Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-26917	Windows Fax Compose Form Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-26918	Windows Fax Compose Form Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-43257	Lack of Neutralization of Formula Elements in the CSV API of MantisBT before 2.25.3 allows an unprivileged attacker to execute code or gain access to information when a user opens the csv_export.php generated CSV file in Excel.	7.8	More Details
CVE-2022-1381	global heap buffer overflow in skip_range in GitHub repository vim/vim prior to 8.2.4763. This vulnerability is capable of crashing software, Bypass Protection Mechanism, Modify Memory, and possible remote execution	7.8	More Details
CVE-2021-21956	A php unserialize vulnerability exists in the Ai-Bolit functionality of CloudLinux Inc Imunify360 5.10.2. A specially-crafted malformed file can lead to potential arbitrary command execution. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2022-26801	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-24473	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26794	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-26793	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-26791	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-27525	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2022-27526	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2022-27188	OS command injection vulnerability exists in CENTUM VP R4.01.00 to R4.03.00, CENTUM VP Small R4.01.00 to R4.03.00, CENTUM VP Basic R4.01.00 to R4.03.00, and B/M9000 VP R6.01.01 to R6.03.02, which may allow an attacker who can access the computer where the affected product is installed to execute an arbitrary OS command by altering a file generated using Graphic Builder.	7.8	More Details
CVE-2022-26790	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-27529	A maliciously crafted PICT, BMP, PSD or TIF file in Autodesk AutoCAD 2022, 2021, 2020, 2019 may be used to write beyond the allocated buffer while parsing PICT, BMP, PSD or TIF file. This vulnerability may be exploited to execute arbitrary code.	7.8	More Details
CVE-2022-26795	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27530	A maliciously crafted TIF or PICT file in Autodesk AutoCAD 2022, 2021, 2020, 2019 can be used to write beyond the allocated buffer through Buffer overflow vulnerability. This vulnerability may be exploited to execute arbitrary code.	7.8	More Details
CVE-2022-1304	An out-of-bounds read/write vulnerability was found in e2fsprogs 1.46.5. This issue leads to a segmentation fault and possibly arbitrary code execution via a specially crafted filesystem.	7.8	More Details
CVE-2022-26796	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-26797	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-26792	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-20692	A vulnerability in the NETCONF over SSH feature of Cisco IOS XE Software could allow a low-privileged, authenticated, remote attacker to cause a denial of service condition (DoS) on an affected device. This vulnerability is due to insufficient resource management. An attacker could exploit this vulnerability by initiating a large number of NETCONF over SSH connections. A successful exploit could allow the attacker to exhaust resources, causing the device to reload and resulting in a DoS condition on an affected device.	7.7	More Details
CVE-2020-25163	A remote attacker with write access to PI ProcessBook files could inject code that is imported into OSIsoft PI Vision 2020 versions prior to 3.5.0. Unauthorized information disclosure, modification, or deletion is also possible if a victim views or interacts with the infected display. This vulnerability affects PI System data and other data accessible with victim’s user permissions.	7.7	More Details
CVE-2015-20107	In Python (aka CPython) up to 3.10.8, the mailcap module does not add escape characters into commands discovered in the system mailcap file. This may allow attackers to inject shell commands into applications that call mailcap.findmatch with untrusted input (if they lack validation of user-provided filenames or arguments). The fix is also back-ported to 3.7, 3.8, 3.9	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25166	An improper verification of the cryptographic signature of firmware updates of the B. Braun Melsungen AG SpaceCom Version L81/U61 and earlier, and the Data module compactplus Versions A10 and A11 allows attackers to generate valid firmware updates with arbitrary content that can be used to tamper with devices.	7.6	More Details
CVE-2020-25150	A relative path traversal attack in the B. Braun Melsungen AG SpaceCom Version L81/U61 and earlier, and the Data module compactplus Versions A10 and A11 allows attackers with service user privileges to upload arbitrary files. By uploading a specially crafted tar file an attacker can execute arbitrary commands.	7.6	More Details
CVE-2020-25158	A reflected cross-site scripting (XSS) vulnerability in the B. Braun Melsungen AG SpaceCom Version L81/U61 and earlier, and the Data module compactplus Versions A10 and A11 allows remote attackers to inject arbitrary web script or HTML into various locations.	7.6	More Details
CVE-2021-44506	An issue was discovered in FIS GT.M through V7.0-000 (related to the YottaDB code base). A lack of input validation in calls to do_verify in sr_unix/do_verify.c allows attackers to attempt to jump to a NULL pointer by corrupting a function pointer.	7.5	More Details
CVE-2021-44507	An issue was discovered in FIS GT.M through V7.0-000 (related to the YottaDB code base). A lack of parameter validation in calls to memcpy in str_tok in sr_unix/ztimeoutroutines.c allows attackers to attempt to read from a NULL pointer.	7.5	More Details
CVE-2021-44510	An issue was discovered in FIS GT.M through V7.0-000 (related to the YottaDB code base). Using crafted input, attackers can cause a calculation of the size of calls to memset in op_fnj3 in sr_port/op_fnj3.c to result in an extremely large value in order to cause a segmentation fault and crash the application.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21476	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. 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 access to critical data or complete access to all 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. 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-2022-21983	Win32 Stream Enumeration Remote Code Execution Vulnerability	7.5	More Details
CVE-2021-44505	An issue was discovered in FIS GT.M through V7.0-000 (related to the YottaDB code base). Using crafted input, an attacker can cause a NULL pointer dereference after calls to ZPrint.	7.5	More Details
CVE-2021-44508	An issue was discovered in FIS GT.M through V7.0-000 (related to the YottaDB code base). A lack of NULL checks in calls to ious_open in sr_unix/ious_open.c allows attackers to crash the application by dereferencing a NULL pointer.	7.5	More Details
CVE-2021-44509	An issue was discovered in FIS GT.M through V7.0-000 (related to the YottaDB code base). Using crafted input, attackers can cause an integer underflow of the size of calls to memset in op_fnj3 in sr_port/op_fnj3.c in order to cause a segmentation fault and crash the application.	7.5	More Details
CVE-2021-44504	An issue was discovered in FIS GT.M through V7.0-000 (related to the YottaDB code base). Using crafted input, an attacker can cause a size variable, stored as an signed int, to equal an extremely large value, which is interpreted as a negative value during a check. This value is then used in a memcpy call on the stack, causing a memory segmentation fault.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44503	An issue was discovered in FIS GT.M through V7.0-000 (related to the YottaDB code base). Using crafted input, an attacker can cause a call to va_arg on an empty variadic parameter list, most likely causing a memory segmentation fault.	7.5	More Details
CVE-2021-44502	An issue was discovered in FIS GT.M through V7.0-000 (related to the YottaDB code base). Using crafted input, an attacker can control the size of a memset that occurs in calls to util_format in sr_unix/util_output.c.	7.5	More Details
CVE-2021-40392	An information disclosure vulnerability exists in the Web Application functionality of Moxa MXView Series 3.2.4. Network sniffing can lead to a disclosure of sensitive information. An attacker can sniff network traffic to exploit this vulnerability.	7.5	More Details
CVE-2022-24485	Win32 File Enumeration Remote Code Execution Vulnerability	7.5	More Details
CVE-2022-26832	.NET Framework Denial of Service Vulnerability	7.5	More Details
CVE-2021-26627	Real-time image information exposure is caused by insufficient authentication for activated RTSP port. This vulnerability could allow to remote attackers to send the RTSP requests using ffplay command and lead to leakage a live image.	7.5	More Details
CVE-2022-24279	The package madlib-object-utils before 0.1.8 are vulnerable to Prototype Pollution via the setValue method, as it allows an attacker to merge object prototypes into it. *Note:* This vulnerability derives from an incomplete fix of [CVE-2020-7701](https://security.snyk.io/vuln/SNYK-JS-MADLIBOBJECTUTILS-598676)	7.5	More Details
CVE-2022-26924	YARP Denial of Service Vulnerability	7.5	More Details
CVE-2022-27008	nginx njs 0.7.2 is vulnerable to Buffer Overflow. Type confused in Array.prototype.concat() when a slow array appended element is fast array.	7.5	More Details
CVE-2022-26915	Windows Secure Channel Denial of Service Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26665	An Insecure Direct Object Reference issue exists in the Tyler Odyssey Portal platform before 17.1.20. This may allow an external party to access sensitive case records.	7.5	More Details
CVE-2022-26831	Windows Lightweight Directory Access Protocol (LDAP) Denial of Service Vulnerability	7.5	More Details
CVE-2022-24534	Win32 Stream Enumeration Remote Code Execution Vulnerability	7.5	More Details
CVE-2022-26830	DiskUsage.exe Remote Code Execution Vulnerability	7.5	More Details
CVE-2022-22183	An Improper Access Control vulnerability in Juniper Networks Junos OS Evolved allows a network-based unauthenticated attacker who is able to connect to a specific open IPv4 port, which in affected releases should otherwise be unreachable, to cause the CPU to consume all resources as more traffic is sent to the port to create a Denial of Service (DoS) condition. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS Evolved 20.4 versions prior to 20.4R3-S2-EVO; 21.1 versions prior to 21.1R3-S1-EVO; 21.2 versions prior to 21.2R3-EVO; 21.3 versions prior to 21.3R2-EVO; 21.4 versions prior to 21.4R2-EVO. This issue does not affect Junos OS.	7.5	More Details
CVE-2022-1339	SQL injection in ElementController.php in GitHub repository pimcore/pimcore prior to 10.3.5. This vulnerability is capable of steal the data	7.5	More Details
CVE-2021-44500	An issue was discovered in FIS GT.M through V7.0-000 (related to the YottaDB code base). A lack of input validation in calls to eb_div in sr_port/eb_muldiv.c allows attackers to crash the application by performing a divide by zero.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22185	A vulnerability in Juniper Networks Junos OS on SRX Series, allows a network-based unauthenticated attacker to cause a Denial of Service (DoS) by sending a specific fragmented packet to the device, resulting in a flowd process crash, which is responsible for packet forwarding. Continued receipt and processing of this specific packet will create a sustained DoS condition. This issue only affects SRX Series when 'preserve-incoming-fragment-size' feature is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 18.3 versions prior to 18.3R3-S6; 18.4 versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R3-S6; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS prior to 17.3R1.	7.5	More Details
CVE-2022-22188	An Uncontrolled Memory Allocation vulnerability leading to a Heap-based Buffer Overflow in the packet forwarding engine (PFE) of Juniper Networks Junos OS allows a network-based unauthenticated attacker to flood the device with traffic leading to a Denial of Service (DoS). The device must be configured with storm control profiling limiting the number of unknown broadcast, multicast, or unicast traffic to be vulnerable to this issue. This issue affects: Juniper Networks Junos OS on QFX5100/QFX5110/QFX5120/QFX5200/QFX5210/EX4600/EX4650 Series; 20.2 version 20.2R1 and later versions prior to 20.2R2. This issue does not affect: Juniper Networks Junos OS versions prior to 20.2R1.	7.5	More Details
CVE-2021-44501	An issue was discovered in FIS GT.M through V7.0-000 (related to the YottaDB code base). Using crafted input, an attacker can cause calls to ZRead to crash due to a NULL pointer dereference.	7.5	More Details
CVE-2022-27257	A PHP Local File Inclusion vulneraility in the default Redbasic theme for Hubzilla before version 7.2 allows remote attackers to include arbitrary php files via the schema parameter.	7.5	More Details
CVE-2021-44499	An issue was discovered in FIS GT.M through V7.0-000 (related to the YottaDB code base). Using crafted input, an attacker can cause a call to $Extract to force an signed integer holding the size of a buffer to take on a large negative number, which is then used as the length of a memcpy call that occurs on the stack, causing a buffer overflow.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22195	An Improper Update of Reference Count vulnerability in the kernel of Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to trigger a counter overflow, eventually causing a Denial of Service (DoS). This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S1-EVO; 21.1 versions prior to 21.1R3-EVO; 21.2 versions prior to 21.2R3-EVO; 21.3 versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS.	7.5	More Details
CVE-2022-28345	The Signal app before 5.34 for iOS allows URI spoofing via RTLO injection. It incorrectly renders RTLO encoded URLs beginning with a non-breaking space, when there is a hash character in the URL. This technique allows a remote unauthenticated attacker to send legitimate looking links, appearing to be any website URL, by abusing the non-http/non-https automatic rendering of URLs. An attacker can spoof, for example, example.com, and masquerade any URL with a malicious destination. An attacker requires a subdomain such as gepj, txt, fdp, or xcod, which would appear backwards as jpeg, txt, pdf, and docx respectively.	7.5	More Details
CVE-2022-27447	MariaDB Server v10.9 and below was discovered to contain a use-after-free via the component Binary_string::free_buffer() at /sql/sql_string.h.	7.5	More Details
CVE-2022-21421	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web General). Supported versions that are affected are 5.5.0.0.0, 5.9.0.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition 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-2021-44498	An issue was discovered in FIS GT.M through V7.0-000 (related to the YottaDB code base). Using crafted input, attackers can cause a type to be incorrectly initialized in the function f_incr in sr_port/f_incr.c and cause a crash due to a NULL pointer dereference.	7.5	More Details
CVE-2022-27448	There is an Assertion failure in MariaDB Server v10.9 and below via 'node->pcur->rel_pos == BTR_PCUR_ON' at /row/row0mysql.cc.	7.5	More Details
CVE-2022-27449	MariaDB Server v10.9 and below was discovered to contain a segmentation fault via the component sql/item_func.cc:148.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24843	Gin-vue-admin is a backstage management system based on vue and gin, which separates the front and rear of the full stack. Gin-vue-admin 2.50 has arbitrary file read vulnerability due to a lack of parameter validation. This has been resolved in version 2.5.1. There are no known workarounds for this issue.	7.5	More Details
CVE-2022-27451	MariaDB Server v10.9 and below was discovered to contain a segmentation fault via the component sql/field_conv.cc.	7.5	More Details
CVE-2022-27452	MariaDB Server v10.9 and below was discovered to contain a segmentation fault via the component sql/item_cmpfunc.cc.	7.5	More Details
CVE-2022-27455	MariaDB Server v10.6.3 and below was discovered to contain an use-after-free in the component my_wildcmp_8bit_impl at /strings/ctype-simple.c.	7.5	More Details
CVE-2022-27456	MariaDB Server v10.6.3 and below was discovered to contain an use-after-free in the component VDec::VDec at /sql/sql_type.cc.	7.5	More Details
CVE-2022-27457	MariaDB Server v10.6.3 and below was discovered to contain an use-after-free in the component my_mb_wc_latin1 at /strings/ctype-latin1.c.	7.5	More Details
CVE-2022-29153	HashiCorp Consul and Consul Enterprise up to 1.9.16, 1.10.9, and 1.11.4 may allow server side request forgery when the Consul client agent follows redirects returned by HTTP health check endpoints. Fixed in 1.9.17, 1.10.10, and 1.11.5.	7.5	More Details
CVE-2022-22198	An Access of Uninitialized Pointer vulnerability in the SIP ALG of Juniper Networks Junos OS allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. On all MX and SRX platforms, if the SIP ALG is enabled, an MS-MPC or MS-MIC, or SPC will crash if it receives a SIP message with a specific contact header format. This issue affects Juniper Networks Junos OS on MX Series and SRX Series: 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect versions prior to 20.4R1.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21422	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Connection Manager). Supported versions that are affected are 12.0.0.4 and 12.0.0.5. Difficult to exploit vulnerability allows low privileged attacker with network access via TCP to compromise Oracle Communications Billing and Revenue Management. Successful attacks of this vulnerability can result in takeover of Oracle Communications Billing and Revenue Management. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	7.5	More Details
CVE-2022-22197	An Operation on a Resource after Expiration or Release vulnerability in the Routing Protocol Daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker with an established BGP session to cause a Denial of Service (DoS). This issue occurs when proxy-generate route-target filtering is enabled, and certain proxy-route add and delete events are happening. This issue affects: Juniper Networks Junos OS All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S8, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S2, 20.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.1R3-EVO; 20.2 versions prior to 20.2R3-EVO; 20.3 versions prior to 20.3R2-EVO.	7.5	More Details
CVE-2021-39076	IBM Security Guardium 10.5 and 11.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt sensitive information. IBM X-Force ID: 215585.	7.5	More Details
CVE-2022-26498	An issue was discovered in Asterisk through 19.x. When using STIR/SHAKEN, it is possible to download files that are not certificates. These files could be much larger than what one would expect to download, leading to Resource Exhaustion. This is fixed in 16.25.2, 18.11.2, and 19.3.2.	7.5	More Details
CVE-2022-27446	MariaDB Server v10.9 and below was discovered to contain a segmentation fault via the component sql/item_cmpfunc.h.	7.5	More Details
CVE-2022-1341	An issue was discovered in in bwm-ng v0.6.2. An arbitrary null write exists in get_cmdln_options() function in src/options.c.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44366	Multiple denial of service vulnerabilities exist in the cgiserver.cgi JSON command parser functionality of Reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. An attacker can send an HTTP request to trigger this vulnerability.	7.5	More Details
CVE-2021-40400	An out-of-bounds read vulnerability exists in the RS-274X aperture macro outline primitive functionality of Gerbv 2.7.0 and dev (commit b5f1eacd) and the forked version of Gerbv (commit d7f42a9a). A specially-crafted Gerber file can lead to information disclosure. An attacker can provide a malicious file to trigger this vulnerability.	7.5	More Details
CVE-2021-40402	An out-of-bounds read vulnerability exists in the RS-274X aperture macro multiple outline primitives functionality of Gerbv 2.7.0 and dev (commit b5f1eacd), and Gerbv forked 2.7.1 and 2.8.0. A specially-crafted Gerber file can lead to information disclosure. An attacker can provide a malicious file to trigger this vulnerability.	7.5	More Details
CVE-2021-43289	An issue was discovered in ThoughtWorks GoCD before 21.3.0. An attacker who has compromised a GoCD agent can upload a malicious file into an arbitrary directory of a GoCD server, but does not control the filename.	7.5	More Details
CVE-2021-44354	Multiple denial of service vulnerabilities exist in the cgiserver.cgi JSON command parser functionality of Reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. An attacker can send an HTTP request to trigger this vulnerability.	7.5	More Details
CVE-2021-44355	Multiple denial of service vulnerabilities exist in the cgiserver.cgi JSON command parser functionality of Reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. An attacker can send an HTTP request to trigger this vulnerability.	7.5	More Details
CVE-2021-44356	Multiple denial of service vulnerabilities exist in the cgiserver.cgi JSON command parser functionality of Reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. An attacker can send an HTTP request to trigger this vulnerability.	7.5	More Details
CVE-2021-44357	Multiple denial of service vulnerabilities exist in the cgiserver.cgi JSON command parser functionality of Reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. An attacker can send an HTTP request to trigger this vulnerability.	7.5	More Details
CVE-2021-44375	Multiple denial of service vulnerabilities exist in the cgiserver.cgi JSON command parser functionality of Reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. An attacker can send an HTTP request to trigger this vulnerability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27445	MariaDB Server v10.9 and below was discovered to contain a segmentation fault via the component sql/sql_window.cc.	7.5	More Details
CVE-2021-44394	Multiple denial of service vulnerabilities exist in the cgiserver.cgi JSON command parser functionality of Reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. An attacker can send an HTTP request to trigger this vulnerability.	7.5	More Details
CVE-2022-1119	The Simple File List WordPress plugin is vulnerable to Arbitrary File Download via the eeFile parameter found in the ~/includes/ee-downloader.php file due to missing controls which makes it possible unauthenticated attackers to supply a path to a file that will subsequently be downloaded, in versions up to and including 3.2.7.	7.5	More Details
CVE-2022-27444	MariaDB Server v10.9 and below was discovered to contain a segmentation fault via the component sql/item_subselect.cc.	7.5	More Details
CVE-2021-43287	An issue was discovered in ThoughtWorks GoCD before 21.3.0. The business continuity add-on, which is enabled by default, leaks all secrets known to the GoCD server to unauthenticated attackers.	7.5	More Details
CVE-2022-24863	http-swagger is an open source wrapper to automatically generate RESTful API documentation with Swagger 2.0. In versions of http-swagger prior to 1.2.6 an attacker may perform a denial of service attack consisting of memory exhaustion on the host system. The cause of the memory exhaustion is down to improper handling of http methods. Users are advised to upgrade. Users unable to upgrade may to restrict the path prefix to the "GET" method as a workaround.	7.5	More Details
CVE-2020-25162	A XPath injection vulnerability in the B. Braun Melsungen AG SpaceCom Version L81/U61 and earlier, and the Data module compactplus Versions A10 and A11 allows unauthenticated remote attackers to access sensitive information and escalate privileges.	7.5	More Details
CVE-2021-28505	On affected Arista EOS platforms, if a VXLAN match rule exists in an IPv4 access-list that is applied to the ingress of an L2 or an L3 port/SVI, the VXLAN rule and subsequent ACL rules in that access list will ignore the specified IP protocol.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21441	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-2021-44491	An issue was discovered in YottaDB through r1.32 and V7.0-000. Using crafted input, attackers can cause a calculation of the size of calls to memset in op_fnj3 in sr_port/op_fnj3.c to result in an extremely large value in order to cause a segmentation fault and crash the application. This is a digs-- calculation.	7.5	More Details
CVE-2022-21466	Vulnerability in the Oracle Commerce Guided Search product of Oracle Commerce (component: Tools and Frameworks). The supported version that is affected is 11.3.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search 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-2021-44495	An issue was discovered in YottaDB through r1.32 and V7.0-000 and FIS GT.M through V7.0-000. Using crafted input, an attacker can cause a NULL pointer dereference after calls to ZPrint.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21449	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 17.0.2 and 18; Oracle GraalVM Enterprise Edition: 21.3.1 and 22.0.0.2. 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 creation, deletion or modification access to critical data or all 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. 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-2022-21159	A denial of service vulnerability exists in the parseNormalModeParameters functionality of MZ Automation GmbH libiec61850 1.5.0. A specially-crafted series of network requests can lead to denial of service. An attacker can send a sequence of malformed iec61850 messages to trigger this vulnerability.	7.5	More Details
CVE-2021-44494	An issue was discovered in YottaDB through r1.32 and V7.0-000 and FIS GT.M through V7.0-000. Using crafted input, an attacker can cause calls to ZRead to crash due to a NULL pointer dereference.	7.5	More Details
CVE-2022-27043	Yearning versions 2.3.1 and 2.3.2 Interstellar GA and 2.3.4 - 2.3.6 Neptune is vulnerable to Directory Traversal.	7.5	More Details
CVE-2022-27055	ecjia-daojia 1.38.1-20210202629 is vulnerable to information leakage via content/apps/installer/classes/Helper.php. When the web program is installed, a new environment file is created, and the database information is recorded, including the database record password. NOTE: the vendor disputes this because the environment file is in the data directory, which is not intended for access by website visitors (only the statics directory can be accessed by website visitors)	7.5	More Details
CVE-2021-44490	An issue was discovered in YottaDB through r1.32 and V7.0-000. Using crafted input, attackers can cause a calculation of the size of calls to memset in op_fnj3 in sr_port/op_fnj3.c to result in an extremely large value in order to cause a segmentation fault and crash the application. This is a "- (digs < 1 ? 1 : digs)" subtraction.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44489	An issue was discovered in YottaDB through r1.32 and V7.0-000. Using crafted input, attackers can cause an integer underflow of the size of calls to memset in op_fnj3 in sr_port/op_fnj3.c in order to cause a segmentation fault and crash the application. This is a "- digs" subtraction.	7.5	More Details
CVE-2021-44492	An issue was discovered in YottaDB through r1.32 and V7.0-000 and FIS GT.M through V7.0-000. Using crafted input, attackers can cause a type to be incorrectly initialized in the function f_incr in sr_port/f_incr.c and cause a crash due to a NULL pointer dereference.	7.5	More Details
CVE-2021-44493	An issue was discovered in YottaDB through r1.32 and V7.0-000 and FIS GT.M through V7.0-000. Using crafted input, an attacker can cause a call to $Extract to force an signed integer holding the size of a buffer to take on a large negative number, which is then used as the length of a memcpy call that occurs on the stack, causing a buffer overflow.	7.5	More Details
CVE-2021-44487	An issue was discovered in YottaDB through r1.32 and V7.0-000. A lack of NULL checks in calls to ious_open in sr_unix/ious_open.c allows attackers to crash the application by dereferencing a NULL pointer.	7.5	More Details
CVE-2021-44481	An issue was discovered in YottaDB through r1.32 and V7.0-000. A lack of parameter validation in calls to memcpy in check_and_set_timeout in sr_unix/ztimeoutroutines.c allows attackers to attempt to read from a NULL pointer.	7.5	More Details
CVE-2021-44485	An issue was discovered in YottaDB through r1.32 and V7.0-000. A lack of NULL checks in trip_gen in sr_port/emit_code.c allows attackers to crash the application by dereferencing a NULL pointer.	7.5	More Details
CVE-2021-44497	An issue was discovered in FIS GT.M through V7.0-000 (related to the YottaDB code base). Using crafted input, can cause the bounds of a for loop to be miscalculated, which leads to a use after free condition a pointer is pushed into previously free memory by the loop.	7.5	More Details
CVE-2021-44482	An issue was discovered in YottaDB through r1.32 and V7.0-000. A lack of input validation in calls to do_verify in sr_unix/do_verify.c allows attackers to attempt to jump to a NULL pointer by corrupting a function pointer.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22194	An Improper Check for Unusual or Exceptional Conditions vulnerability in the packetIO daemon of Juniper Networks Junos OS Evolved on PTX10003, PTX10004, and PTX10008 allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). Continued receipt of these crafted packets will cause a sustained Denial of Service condition. This issue affects Juniper Networks Junos OS Evolved all versions prior to 20.4R2-S3-EVO on PTX10003, PTX10004, and PTX10008. This issue does not affect: Juniper Networks Junos OS Evolved versions 21.1R1-EVO and above; Juniper Networks Junos OS.	7.5	More Details
CVE-2021-44483	An issue was discovered in YottaDB through r1.32 and V7.0-000. A lack of input validation in calls to eb_div in sr_port/eb_muldiv.c allows attackers to crash the application by performing a divide by zero.	7.5	More Details
CVE-2021-44484	An issue was discovered in YottaDB through r1.32 and V7.0-000. A lack of NULL checks in calls to emit_trip in sr_port/emit_code.c allows attackers to crash the application by dereferencing a NULL pointer.	7.5	More Details
CVE-2022-27048	A vulnerability has been discovered in Moxa MGate which allows an attacker to perform a man-in-the-middle (MITM) attack on the device. This affects MGate MB3170 Series Firmware Version 4.2 or lower. and MGate MB3270 Series Firmware Version 4.2 or lower. and MGate MB3280 Series Firmware Version 4.1 or lower. and MGate MB3480 Series Firmware Version 3.2 or lower.	7.4	More Details
CVE-2022-20684	A vulnerability in Simple Network Management Protocol (SNMP) trap generation for wireless clients of Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Family could allow an unauthenticated, adjacent attacker to cause an affected device to unexpectedly reload, resulting in a denial of service (DoS) condition on the device. This vulnerability is due to a lack of input validation of the information used to generate an SNMP trap related to a wireless client connection event. An attacker could exploit this vulnerability by sending an 802.1x packet with crafted parameters during the wireless authentication setup phase of a connection. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22190	An Improper Access Control vulnerability in the Juniper Networks Paragon Active Assurance Control Center allows an unauthenticated attacker to leverage a crafted URL to generate PDF reports, potentially containing sensitive configuration information. A feature was introduced in version 3.1 of the Paragon Active Assurance Control Center which allows users to selective share account data using a unique identifier. Knowing the proper format of the URL and the identifier of an existing object in an application it is possible to get access to that object without being logged in, even if the object is not shared, resulting in the opportunity for malicious exfiltration of user data. Note that the Paragon Active Assurance Control Center SaaS offering is not affected by this issue. This issue affects Juniper Networks Paragon Active Assurance version 3.1.0.	7.4	More Details
CVE-2022-20761	A vulnerability in the integrated wireless access point (AP) packet processing of the Cisco 1000 Series Connected Grid Router (CGR1K) could allow an unauthenticated, adjacent attacker to cause a denial of service condition on an affected device. This vulnerability is due to insufficient input validation of received traffic. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the integrated AP to stop processing traffic, resulting in a DoS condition. It may be necessary to manually reload the CGR1K to restore AP operation.	7.4	More Details
CVE-2019-6834	A CWE-502: Deserialization of Untrusted Data vulnerability exists which could allow an attacker to execute arbitrary code on the targeted system with SYSTEM privileges when placing a malicious user to be authenticated for this vulnerability to be successfully exploited. Affected Product: Schneider Electric Software Update (SESU) SUT Service component (V2.1.1 to V2.3.0)	7.3	More Details
CVE-2022-24857	django-mfa3 is a library that implements multi factor authentication for the django web framework. It achieves this by modifying the regular login view. Django however has a second login view for its admin area. This second login view was not modified, so the multi factor authentication can be bypassed. Users are affected if they have activated both django-mfa3 (< 0.5.0) and django.contrib.admin and have not taken any other measures to prevent users from accessing the admin login view. The issue has been fixed in django-mfa3 0.5.0. It is possible to work around the issue by overwriting the admin login route, e.g. by adding the following URL definition *before* the admin routes: url('admin/login/', lambda request: redirect(settings.LOGIN_URL)	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22189	An Incorrect Ownership Assignment vulnerability in Juniper Networks Contrail Service Orchestration (CSO) allows a locally authenticated user to have their permissions elevated without authentication thereby taking control of the local system they are currently authenticated to. This issue affects: Juniper Networks Contrail Service Orchestration 6.0.0 versions prior to 6.0.0 Patch v3 on On-premises installations. This issue does not affect Juniper Networks Contrail Service Orchestration On-premises versions prior to 6.0.0.	7.3	More Details
CVE-2022-26921	Visual Studio Code Elevation of Privilege Vulnerability	7.3	More Details
CVE-2022-20739	A vulnerability in the CLI of Cisco SD-WAN vManage Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system as the root user. The attacker must be authenticated on the affected system as a low-privileged user to exploit this vulnerability. This vulnerability exists because a file leveraged by a root user is executed when a low-privileged user runs specific commands on an affected system. An attacker could exploit this vulnerability by injecting arbitrary commands to a specific file as a lower-privileged user and then waiting until an admin user executes specific commands. The commands would then be executed on the device by the root user. A successful exploit could allow the attacker to escalate their privileges on the affected system from a low-privileged user to the root user.	7.3	More Details
CVE-2022-22958	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain two remote code execution vulnerabilities (CVE-2022-22957 & CVE-2022-22958). A malicious actor with administrative access can trigger deserialization of untrusted data through malicious JDBC URI which may result in remote code execution.	7.2	More Details
CVE-2022-26898	Azure Site Recovery Remote Code Execution Vulnerability	7.2	More Details
CVE-2022-27366	Cscms Music Portal System v4.2 was discovered to contain a blind SQL injection vulnerability via the component dance_Dance.php_hy.	7.2	More Details
CVE-2022-27369	Cscms Music Portal System v4.2 was discovered to contain a SQL injection vulnerability via the component news_News.php_hy.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26811	Windows DNS Server Remote Code Execution Vulnerability	7.2	More Details
CVE-2022-26812	Windows DNS Server Remote Code Execution Vulnerability	7.2	More Details
CVE-2022-26813	Windows DNS Server Remote Code Execution Vulnerability	7.2	More Details
CVE-2022-26815	Windows DNS Server Remote Code Execution Vulnerability	7.2	More Details
CVE-2022-22957	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain two remote code execution vulnerabilities (CVE-2022-22957 & CVE-2022-22958). A malicious actor with administrative access can trigger deserialization of untrusted data through malicious JDBC URI which may result in remote code execution.	7.2	More Details
CVE-2020-13590	Multiple exploitable SQL injection vulnerabilities exist in the 'entities/fields' page of the Rukovoditel Project Management App 2.7.2. A specially crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger these vulnerabilities, this can be done either with administrator credentials or through cross-site request forgery.	7.2	More Details
CVE-2021-46122	Tp-Link TL-WR840N (EU) v6.20 Firmware (0.9.1 4.17 v0001.0 Build 201124 Rel.64328n) is vulnerable to Buffer Overflow via the Password reset feature.	7.2	More Details
CVE-2022-27367	Cscms Music Portal System v4.2 was discovered to contain a SQL injection vulnerability via the component dance_Topic.php_del.	7.2	More Details
CVE-2022-27368	Cscms Music Portal System v4.2 was discovered to contain a SQL injection vulnerability via the component dance_Lists.php_zhuan.	7.2	More Details
CVE-2022-26826	Windows DNS Server Remote Code Execution Vulnerability	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26823	Windows DNS Server Remote Code Execution Vulnerability	7.2	More Details
CVE-2020-25156	Active debug code in the B. Braun Melsungen AG SpaceCom Version L8/U61, and the Data module compactplus Versions A10 and A11 and earlier enables attackers in possession of cryptographic material to access the device as root.	7.2	More Details
CVE-2022-26824	Windows DNS Server Remote Code Execution Vulnerability	7.2	More Details
CVE-2022-1037	The EXMAGE WordPress plugin before 1.0.7 does to ensure that images added via URLs are external images, which could lead to a blind SSRF issue by using local URLs	7.2	More Details
CVE-2022-24536	Windows DNS Server Remote Code Execution Vulnerability	7.2	More Details
CVE-2022-24847	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. The GeoServer security mechanism can perform an unchecked JNDI lookup, which in turn can be used to perform class deserialization and result in arbitrary code execution. The same can happen while configuring data stores with data sources located in JNDI, or while setting up the disk quota mechanism. In order to perform any of the above changes, the attack needs to have obtained admin rights and use either the GeoServer GUI, or its REST API. The lookups are going to be restricted in GeoServer 2.21.0, 2.20.4, 1.19.6. Users unable to upgrade should restrict access to the `geoserver/web` and `geoserver/rest` via a firewall and ensure that the GeoWebCache is not remotely accessible.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22186	Due to an Improper Initialization vulnerability in Juniper Networks Junos OS on EX4650 devices, packets received on the management interface (em0) but not destined to the device, may be improperly forwarded to an egress interface, instead of being discarded. Such traffic being sent by a client may appear genuine, but is non-standard in nature and should be considered as potentially malicious. This issue affects: Juniper Networks Junos OS on EX4650 Series: All versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2; 22.1 versions prior to 22.1R1.	7.2	More Details
CVE-2022-26151	Citrix XenMobile Server 10.12 through RP11, 10.13 through RP7, and 10.14 through RP4 allows Command Injection.	7.2	More Details
CVE-2022-21410	Vulnerability in the Oracle Database - Enterprise Edition Sharding component of Oracle Database Server. The supported version that is affected is 19c. Easily exploitable vulnerability allows high privileged attacker having Create Any Procedure privilege with network access via Oracle Net to compromise Oracle Database - Enterprise Edition Sharding. Successful attacks of this vulnerability can result in takeover of Oracle Database - Enterprise Edition Sharding. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2022-26825	Windows DNS Server Remote Code Execution Vulnerability	7.2	More Details
CVE-2022-27474	SuiteCRM v7.11.23 was discovered to allow remote code execution via a crafted payload injected into the FirstName text field.	7.2	More Details
CVE-2022-28113	An issue in upload.csp of FANTEC GmbH MWiD25-DS Firmware v2.000.030 allows attackers to write files and reset the user passwords without having a valid session cookie.	7.2	More Details
CVE-2022-27421	Chamilo LMS v1.11.13 lacks validation on the user modification form, allowing attackers to escalate privileges to Platform Admin.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27365	Cscms Music Portal System v4.2 was discovered to contain a SQL injection vulnerability via the component dance_Dance.php_del.	7.2	More Details
CVE-2022-22966	An authenticated, high privileged malicious actor with network access to the VMware Cloud Director tenant or provider may be able to exploit a remote code execution vulnerability to gain access to the server.	7.2	More Details
CVE-2022-0661	The Ad Injection WordPress plugin through 1.2.0.19 does not properly sanitize the body of the adverts injected into the pages, allowing a high privileged user (Admin+) to inject arbitrary HTML or javascript even with unfiltered_html disallowed, leading to a stored cross-site scripting (XSS) vulnerability. Further it is also possible to inject PHP code, leading to a Remote Code execution (RCE) vulnerability, even if the DISALLOW_FILE_EDIT and DISALLOW_FILE_MOD constants are both set.	7.2	More Details
CVE-2022-24788	Vyper is a pythonic Smart Contract Language for the ethereum virtual machine. Versions of vyper prior to 0.3.2 suffer from a potential buffer overrun. Importing a function from a JSON interface which returns `bytes` generates bytecode which does not clamp bytes length, potentially resulting in a buffer overrun. Users are advised to upgrade. There are no known workarounds for this issue.	7.1	More Details
CVE-2022-27524	An out-of-bounds read can be exploited in Autodesk TrueView 2022 may lead to an exposure of sensitive information or a crash through using a maliciously crafted DWG file as an Input. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.1	More Details
CVE-2022-29458	ncurses 6.3 before patch 20220416 has an out-of-bounds read and segmentation violation in convert_strings in tinfo/read_entry.c in the terminfo library.	7.1	More Details
CVE-2022-27523	A buffer over-read can be exploited in Autodesk TrueView 2022 may lead to an exposure of sensitive information or a crash through using a maliciously crafted DWG file as an Input. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.1	More Details
CVE-2022-26904	Windows User Profile Service Elevation of Privilege Vulnerability	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26828	Windows Bluetooth Driver Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-26827	Windows File Server Resource Management Service Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-24495	Windows Direct Show Remote Code Execution Vulnerability	7.0	More Details
CVE-2022-26808	Windows File Explorer Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-25165	An issue was discovered in Amazon AWS VPN Client 2.0.0. A TOCTOU race condition exists during the validation of VPN configuration files. This allows parameters outside of the AWS VPN Client allow list to be injected into the configuration file prior to the AWS VPN Client service (running as SYSTEM) processing the file. Dangerous arguments can be injected by a low-level user such as log, which allows an arbitrary destination to be specified for writing log files. This leads to an arbitrary file write as SYSTEM with partial control over the files content. This can be abused to cause an elevation of privilege or denial of service.	7.0	More Details
CVE-2022-24540	Windows ALPC Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-24482	Windows ALPC Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-26807	Windows Work Folder Service Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-28810	Zoho ManageEngine ADSelfService Plus before build 6122 allows a remote authenticated administrator to execute arbitrary operating OS commands as SYSTEM via the policy custom script feature. Due to the use of a default administrator password, attackers may be able to abuse this functionality with minimal effort. Additionally, a remote and partially authenticated attacker may be able to inject arbitrary commands into the custom script due to an unsanitized password field.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20694	A vulnerability in the implementation of the Resource Public Key Infrastructure (RPKI) feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause the Border Gateway Protocol (BGP) process to crash, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of a specific RPKI to Router (RTR) Protocol packet header. An attacker could exploit this vulnerability by compromising the RPKI validator server and sending a specifically crafted RTR packet to an affected device. Alternatively, the attacker could use man-in-the-middle techniques to impersonate the RPKI validator server and send a crafted RTR response packet over the established RTR TCP connection to the affected device. A successful exploit could allow the attacker to cause a DoS condition because the BGP process could constantly restart and BGP routing could become unstable.	6.8	More Details
CVE-2022-20758	A vulnerability in the implementation of the Border Gateway Protocol (BGP) Ethernet VPN (EVPN) functionality in Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. This vulnerability is due to the incorrect processing of a BGP update message that contains specific EVPN attributes. An attacker could exploit this vulnerability by sending a BGP update message that contains specific EVPN attributes. To exploit this vulnerability, an attacker must control a BGP speaker that has an established trusted peer connection to an affected device that is configured with the address family L2VPN EVPN to receive and process the update message. This vulnerability cannot be exploited by any data that is initiated by clients on the Layer 2 network or by peers that are not configured to accept the L2VPN EVPN address family. A successful exploit could allow the attacker to cause the BGP process to restart unexpectedly, resulting in a DoS condition. The Cisco implementation of BGP accepts incoming BGP updates only from explicitly defined peers. For this vulnerability to be exploited, the malicious BGP update message must either come from a configured, valid BGP peer or be injected by the attacker into the affected BGP network on an existing, valid TCP connection to a BGP peer.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20679	A vulnerability in the IPSec decryption routine of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to buffer exhaustion that occurs while traffic on a configured IPsec tunnel is being processed. An attacker could exploit this vulnerability by sending traffic to an affected device that has a maximum transmission unit (MTU) of 1800 bytes or greater. A successful exploit could allow the attacker to cause the device to reload. To exploit this vulnerability, the attacker may need access to the trusted network where the affected device is in order to send specific packets to be processed by the device. All network devices between the attacker and the affected device must support an MTU of 1800 bytes or greater. This access requirement could limit the possibility of a successful exploit.	6.8	More Details
CVE-2020-25160	Improper access controls in the B. Braun Melsungen AG SpaceCom Version L81/U61 and earlier, and the Data module compactplus Versions A10 and A11 enables attackers to extract and tamper with the devices network configuration.	6.8	More Details
CVE-2020-16238	A vulnerability in the configuration import mechanism of the B. Braun Melsungen AG SpaceCom Version L81/U61 and earlier, and the Data module compactplus Versions A10 and A11 allows attackers with command line access to the underlying Linux system to escalate privileges to the root user.	6.7	More Details
CVE-2022-21465	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.34. Easily exploitable vulnerability allows high 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 ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox as well as unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.7 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:L/A:H).	6.7	More Details
CVE-2022-26821	Windows DNS Server Remote Code Execution Vulnerability	6.6	More Details
CVE-2022-26822	Windows DNS Server Remote Code Execution Vulnerability	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26818	Windows DNS Server Remote Code Execution Vulnerability	6.6	More Details
CVE-2022-26814	Windows DNS Server Remote Code Execution Vulnerability	6.6	More Details
CVE-2022-26817	Windows DNS Server Remote Code Execution Vulnerability	6.6	More Details
CVE-2022-26820	Windows DNS Server Remote Code Execution Vulnerability	6.6	More Details
CVE-2022-26829	Windows DNS Server Remote Code Execution Vulnerability	6.6	More Details
CVE-2022-26819	Windows DNS Server Remote Code Execution Vulnerability	6.6	More Details
CVE-2021-43129	A bypass exists for Desire2Learn/D2L Brightspace's "Disable Right Click" option in the quizzing feature, which allows a quiz-taker to access print and copy functionality via the browser's right click menu even when "Disable Right Click" is enabled on the quiz.	6.5	More Details
CVE-2022-21447	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 low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise CS Academic Advisement. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise CS Academic Advisement accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2022-1365	Exposure of Private Personal Information to an Unauthorized Actor in GitHub repository lquixada/cross-fetch prior to 3.1.5.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39033	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.5 and 6.1.0.0 through 6.1.1.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 213963.	6.5	More Details
CVE-2022-23975	Cross-Site Request Forgery (CSRF) in Access Demo Importer <= 1.0.7 on WordPress allows an attacker to activate any installed plugin.	6.5	More Details
CVE-2022-21471	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.34. 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 ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).	6.5	More Details
CVE-2022-24841	fleetdm/fleet is an open source device management, built on osquery. All versions of fleet making use of the teams feature are affected by this authorization bypass issue. Fleet instances without teams, or with teams but without restricted team accounts are not affected. In affected versions a team admin can erroneously add themselves as admin, maintainer or observer on other teams. Users are advised to upgrade to version 4.13. There are no known workarounds for this issue.	6.5	More Details
CVE-2011-1762	A flaw exists in Wordpress related to the 'wp-admin/press-this.php 'script improperly checking user permissions when publishing posts. This may allow a user with 'Contributor-level' privileges to post as if they had 'publish_posts' permission.	6.5	More Details
CVE-2022-21454	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 5.7.37 and prior and 8.0.28 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 Number	Description	Base Score	Reference
CVE-2021-3652	A flaw was found in 389-ds-base. If an asterisk is imported as password hashes, either accidentally or maliciously, then instead of being inactive, any password will successfully match during authentication. This flaw allows an attacker to successfully authenticate as a user whose password was disabled.	6.5	More Details
CVE-2022-21498	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 19c and 21c. Easily exploitable vulnerability allows low privileged attacker having Create Procedure privilege with network access via multiple protocols to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java VM accessible data. CVSS 3.1 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N).	6.5	More Details
CVE-2022-21467	Vulnerability in the Oracle Agile PLM product of Oracle Supply Chain (component: Attachments). The supported version that is affected is 9.3.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Agile PLM accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2022-26783	Windows Hyper-V Shared Virtual Hard Disks Information Disclosure Vulnerability	6.5	More Details
CVE-2020-25164	A vulnerability in the B. Braun Melsungen AG SpaceCom Version L81/U61 and earlier, and the Data module compactplus Versions A10 and A11 allows attackers to recover user credentials of the administrative interface.	6.5	More Details
CVE-2022-24538	Windows Cluster Shared Volume (CSV) Denial of Service Vulnerability	6.5	More Details
CVE-2022-26784	Windows Cluster Shared Volume (CSV) Denial of Service Vulnerability	6.5	More Details
CVE-2022-26589	A Cross-Site Request Forgery (CSRF) in Pluck CMS v4.7.15 allows attackers to delete arbitrary pages.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26785	Windows Hyper-V Shared Virtual Hard Disks Information Disclosure Vulnerability	6.5	More Details
CVE-2022-26816	Windows DNS Server Information Disclosure Vulnerability	6.5	More Details
CVE-2022-23268	Windows Hyper-V Denial of Service Vulnerability	6.5	More Details
CVE-2022-20747	A vulnerability in the History API of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to gain access to sensitive information on an affected system. This vulnerability is due to insufficient API authorization checking on the underlying operating system. An attacker could exploit this vulnerability by sending a crafted API request to Cisco vManage as a lower-privileged user and gaining access to sensitive information that they would not normally be authorized to access.	6.5	More Details
CVE-2022-20735	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface on an affected system. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user. These actions could include modifying the system configuration and deleting accounts.	6.5	More Details
CVE-2022-28041	stb_image.h v2.27 was discovered to contain an integer overflow via the function stbi__jpeg_decode_block_prog_dc. This vulnerability allows attackers to cause a Denial of Service (DoS) via unspecified vectors.	6.5	More Details
CVE-2022-24849	DisCatSharp is a Discord API wrapper for .NET. Users of versions 9.8.5, 9.8.6, 9.9.0 and previously published prereleases of 10.0.0 who have used either one of the two `RequireDisCatSharpDeveloperAttribute`s or the `BaseDiscordClient.LibraryDeveloperTeam` have potentially had their bot token sent to a web server not affiliated with Discord. This server is owned and operated by DisCatSharp's development team. The tokens were not logged, yet it is still advisable to reset the tokens of potentially affected bots. 9.9.1 has been released to patch the issue for the current stable release and the current 10.0.0 prereleases are also no longer affected. Users unable to upgrade should remove all uses of the two `RequireDisCatSharpDeveloperAttribute`s and all direct calls to `BaseDiscordClient.LibraryDeveloperTeam`.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25152	A session fixation vulnerability in the B. Braun Melsungen AG SpaceCom administrative interface Version L81/U61 and earlier, and the Data module compactplus Versions A10 and A11 allows remote attackers to hijack web sessions and escalate privileges.	6.5	More Details
CVE-2022-26911	Skype for Business Information Disclosure Vulnerability	6.5	More Details
CVE-2021-40425	An out-of-bounds read vulnerability exists in the IOCTL GetProcessCommand and B_03 of Webroot Secure Anywhere 21.4. A specially-crafted executable can lead to denial of service. An attacker can issue an ioctl to trigger this vulnerability. An out-of-bounds read vulnerability exists in the IOCTL GetProcessCommand and B_03 of Webroot Secure Anywhere 21.4. An IOCTL_B03 request with specific invalid data causes a similar issue in the device driver WRCore_x64. An attacker can issue an ioctl to trigger this vulnerability.	6.5	More Details
CVE-2021-40424	An out-of-bounds read vulnerability exists in the IOCTL GetProcessCommand and B_03 of Webroot Secure Anywhere 21.4. A specially-crafted executable can lead to denial of service. An attacker can issue an ioctl to trigger this vulnerability. An out-of-bounds read vulnerability exists in the IOCTL GetProcessCommand and B_03 of Webroot Secure Anywhere 21.4. The GetProcessCommandLine IOCTL request could cause an out-of-bounds read in the device driver WRCore_x64. An attacker can issue an ioctl to trigger this vulnerability.	6.5	More Details
CVE-2021-40405	A denial of service vulnerability exists in the cgiserver.cgi Upgrade API functionality of Reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. An attacker can send an HTTP request to trigger this vulnerability.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22196	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent, unauthenticated attacker with an established ISIS adjacency to cause a Denial of Service (DoS). The rpd CPU spikes to 100% after a malformed ISIS TLV has been received which will lead to processing issues of routing updates and in turn traffic impact. This issue affects: Juniper Networks Junos OS 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R2-S6, 19.4R3-S6; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.2 versions prior to 21.2R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1.	6.5	More Details
CVE-2022-22191	A Denial of Service (DoS) vulnerability in the processing of a flood of specific ARP traffic in Juniper Networks Junos OS on the EX4300 switch, sent from the local broadcast domain, may allow an unauthenticated network-adjacent attacker to trigger a PFEMAN watchdog timeout, causing the Packet Forwarding Engine (PFE) to crash and restart. After the restart, transit traffic will be temporarily interrupted until the PFE is reprogrammed. In a virtual chassis (VC), the impacted Flexible PIC Concentrator (FPC) may split from the VC temporarily, and join back into the VC once the PFE restarts. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on the EX4300: All versions prior to 15.1R7-S12; 18.4 versions prior to 18.4R2-S10, 18.4R3-S11; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S9, 19.2R3-S4; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2-S1, 21.2R3; 21.3 versions prior to 21.3R1-S2, 21.3R2.	6.5	More Details
CVE-2022-1279	A vulnerability in the encryption implementation of EBICS messages in the open source librairy ebics-java/ebics-java-client allows an attacker sniffing network traffic to decrypt EBICS payloads. This issue affects: ebics-java/ebics-java-client versions prior to 1.2.	6.5	More Details
CVE-2022-24498	Windows iSCSI Target Service Information Disclosure Vulnerability	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21490	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.35 and prior, 7.5.25 and prior, 7.6.21 and prior and 8.0.28 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-2022-21489	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.35 and prior, 7.5.25 and prior, 7.6.21 and prior and 8.0.28 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-2022-21483	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.35 and prior, 7.5.25 and prior, 7.6.21 and prior and 8.0.28 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 Number	Description	Base Score	Reference
CVE-2022-21482	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.28 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-2022-1280	A use-after-free vulnerability was found in drm_lease_held in drivers/gpu/drm/drm_lease.c in the Linux kernel due to a race problem. This flaw allows a local user privilege attacker to cause a denial of service (DoS) or a kernel information leak.	6.3	More Details
CVE-2022-24859	PyPDF2 is an open source python PDF library capable of splitting, merging, cropping, and transforming the pages of PDF files. In versions prior to 1.27.5 an attacker who uses this vulnerability can craft a PDF which leads to an infinite loop if the PyPDF2 if the code attempts to get the content stream. The reason is that the last while-loop in `ContentStream._readInlineImage` only terminates when it finds the `EI` token, but never actually checks if the stream has already ended. This issue has been resolved in version `1.27.5`. Users unable to upgrade should validate and PDFs prior to iterating over their content stream.	6.2	More Details
CVE-2022-24858	next-auth v3 users before version 3.29.2 are impacted. next-auth version 4 users before version 4.3.2 are also impacted. Upgrading to 3.29.2 or 4.3.2 will patch this vulnerability. If you are not able to upgrade for any reason, you can add a configuration to your callbacks option. If you already have a `redirect` callback, make sure that you match the incoming `url` origin against the `baseUrl`.	6.1	More Details
CVE-2022-28221	The CleanTalk AntiSpam plugin <= 5.173 for WordPress is vulnerable to Reflected Cross-Site Scripting (XSS) via the $_REQUEST['page'] parameter in`/lib/Cleantalk/ApbctWP/FindSpam/ListTable/Comments.php`	6.1	More Details
CVE-2022-27422	A reflected cross-site scripting (XSS) vulnerability in Chamilo LMS v1.11.13 allows attackers to execute arbitrary web scripts or HTML via user interaction with a crafted URL.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21409	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime). The supported version that is affected is Prior to 9.2.6.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, 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 JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2022-0780	The SearchIQ WordPress plugin before 3.9 contains a flag to disable the verification of CSRF nonces, granting unauthenticated attackers access to the siq_ajax AJAX action and allowing them to perform Cross-Site Scripting attacks due to the lack of sanitisation and escaping in the customCss parameter	6.1	More Details
CVE-2022-1231	XSS via Embedded SVG in SVG Diagram Format in GitHub repository plantuml/plantuml prior to 1.2022.4. Stored XSS in the context of the diagram embedder. Depending on the actual context, this ranges from stealing secrets to account hijacking or even to code execution for example in desktop applications. Web based applications are the ones most affected. Since the SVG format allows clickable links in diagrams, it is commonly used in plugins for web based projects (like the Confluence plugin, etc. see https://plantuml.com/de/running).	6.1	More Details
CVE-2022-29020	ForestBlog through 2022-02-16 allows admin/profile/save userAvatar XSS during addition of a user avatar.	6.1	More Details
CVE-2022-1187	The WordPress WP YouTube Live Plugin is vulnerable to Reflected Cross-Site Scripting via POST data found in the ~/inc/admin.php file which allows unauthenticated attackers to inject arbitrary web scripts in versions up to, and including, 1.7.21.	6.1	More Details
CVE-2022-27475	Cross site scripting (XSS) vulnerability in tramyardg hotel-mgmt-system, allows attackers to execute arbitrary code when when /admin.php is loaded.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29653	Froxlor through 0.10.22 does not perform validation on user input passed in the customermail GET parameter. The value of this parameter is reflected in the login webpage, allowing the injection of arbitrary HTML tags.	6.1	More Details
CVE-2022-28222	The CleanTalk AntiSpam plugin <= 5.173 for WordPress is vulnerable to Reflected Cross-Site Scripting (XSS) via the $_REQUEST['page'] parameter in`/lib/Cleantalk/ApbctWP/FindSpam/ListTable/Users.php`	6.1	More Details
CVE-2022-1257	Insecure storage of sensitive information vulnerability in MA for Linux, macOS, and Windows prior to 5.7.6 allows a local user to gain access to sensitive information through storage in ma.db. The sensitive information has been moved to encrypted database files.	6.1	More Details
CVE-2021-43154	Cross Site Scripting (XSS) vulnerability exists in CMS Made Simple 2.2.15 via the Name field in an Add Category action in moduleinterface.php.	6.1	More Details
CVE-2022-27256	A PHP Local File inclusion vulnerability in the Redbasic theme for Hubzilla before version 7.2 allows remote attackers to include arbitrary php files via the schema parameter.	6.1	More Details
CVE-2022-27425	Chamilo LMS v1.11.13 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /blog/blog.php.	6.1	More Details
CVE-2022-21492	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Server). The supported version that is affected is 5.9.0.0.0. Easily exploitable vulnerability allows unauthenticated 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 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2022-0645	Open redirect vulnerability via endpoint authorize_and_redirect/?redirect= in GitHub repository posthog/posthog prior to 1.34.1.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26144	An XSS issue was discovered in MantisBT before 2.25.3. Improper escaping of a Plugin name allows execution of arbitrary code (if CSP allows it) in manage_plugin_page.php and manage_plugin_uninstall.php when a crafted plugin is installed.	6.1	More Details
CVE-2022-1383	Heap-based Buffer Overflow in GitHub repository radareorg/radare2 prior to 5.6.8. The bug causes the program reads data past the end of the intented buffer. Typically, this can allow attackers to read sensitive information from other memory locations or cause a crash.	6.1	More Details
CVE-2021-25120	The Easy Social Feed Free and Pro WordPress plugins before 6.2.7 do not sanitise some of their parameters used via AJAX actions before outputting them back in the response, leading to Reflected Cross-Site Scripting issues	6.1	More Details
CVE-2022-1091	The sanitisation step of the Safe SVG WordPress plugin before 1.9.10 can be bypassed by spoofing the content-type in the POST request to upload a file. Exploiting this vulnerability, an attacker will be able to perform the kinds of attacks that this plugin should prevent (mainly XSS, but depending on further use of uploaded SVG files potentially other XML attacks).	6.1	More Details
CVE-2022-21468	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Popups). Supported versions that are affected are 12.2.4-12.2.11. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Framework, 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 Applications Framework accessible data as well as unauthorized read access to a subset of Oracle Applications Framework accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21419	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Visual Analyzer). Supported versions that are affected are 5.5.0.0.0 and 5.9.0.0.0. Easily exploitable vulnerability allows unauthenticated 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 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2022-0879	The Caldera Forms WordPress plugin before 1.9.7 does not validate and escape the cf-api parameter before outputting it back in the response, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-21453	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). 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 require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, 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 WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2022-27503	Cross-site Scripting (XSS) vulnerability in Citrix StoreFront affects version 1912 before CU5 and version 3.12 before CU9	6.1	More Details
CVE-2022-27852	Multiple Unauthenticated Stored Cross-Site Scripting (XSS) vulnerabilities in KB Support (WordPress plugin) <= 1.5.5 versions.	6.1	More Details
CVE-2022-27258	Multiple Cross-Site Scripting (XSS) vulnerabilities in Hubzilla 7.0.3 and earlier allows remote attacker to include arbitrary web script or HTML via the rpath parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26594	Multiple cross-site scripting (XSS) vulnerabilities in Liferay Portal 7.3.5 through 7.4.0, and Liferay DXP 7.3 before service pack 3 allow remote attackers to inject arbitrary web script or HTML via a form field's help text to (1) Forms module's form builder, or (2) App Builder module's object form view's form builder.	6.1	More Details
CVE-2022-21458	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Navigation Pages, Portal, Query). Supported versions that are affected are 8.58 and 8.59. Easily exploitable vulnerability allows unauthenticated 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 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2022-21448	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Visual Analyzer). The supported version that is affected is 5.9.0.0.0. Easily exploitable vulnerability allows unauthenticated 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 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21456	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Navigation Pages, Portal, Query). Supported versions that are affected are 8.58 and 8.59. Easily exploitable vulnerability allows unauthenticated 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 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2022-27505	Reflected cross site scripting (XSS)	6.1	More Details
CVE-2022-21470	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Process Scheduler). Supported versions that are affected are 8.58 and 8.59. Easily exploitable vulnerability allows unauthenticated 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 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21480	Vulnerability in the Oracle Transportation Management product of Oracle Supply Chain (component: User Interface). Supported versions that are affected are 6.4.3 and 6.5.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Transportation Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Transportation Management, 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 Transportation Management accessible data as well as unauthorized read access to a subset of Oracle Transportation Management accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2022-21493	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes 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 ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:N/I:N/A:H).	5.9	More Details
CVE-2022-21475	Vulnerability in the Oracle Banking Payments product of Oracle Financial Services Applications (component: Infrastructure). The supported version that is affected is 14.5. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. 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 Banking Payments accessible data as well as unauthorized read access to a subset of Oracle Banking Payments accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Payments. CVSS 3.1 Base Score 5.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:H/A:L).	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21457	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PAM Auth Plugin). Supported versions that are affected are 8.0.28 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	5.9	More Details
CVE-2022-24853	Metabase is an open source business intelligence and analytics application. Metabase has a proxy to load arbitrary URLs for JSON maps as part of our GeoJSON support. While we do validation to not return contents of arbitrary URLs, there is a case where a particularly crafted request could result in file access on windows, which allows enabling an `NTLM relay attack`, potentially allowing an attacker to receive the system password hash. If you use Windows and are on this version of Metabase, please upgrade immediately. The following patches (or greater versions) are available: 0.42.4 and 1.42.4, 0.41.7 and 1.41.7, 0.40.8 and 1.40.8.	5.9	More Details
CVE-2022-21474	Vulnerability in the Oracle Banking Trade Finance product of Oracle Financial Services Applications (component: Infrastructure). The supported version that is affected is 14.5. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Trade Finance. 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 Banking Trade Finance accessible data as well as unauthorized read access to a subset of Oracle Banking Trade Finance accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Trade Finance. CVSS 3.1 Base Score 5.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:H/A:L).	5.9	More Details
CVE-2021-21967	An out-of-bounds write vulnerability exists in the OTA update task functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. A specially-crafted MQTT payload can lead to denial of service. An attacker can perform a man-in-the-middle attack to trigger this vulnerability.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21472	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 12.4, 14.0-14.3 and 14.5. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. 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 FLEXCUBE Universal Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Universal Banking. CVSS 3.1 Base Score 5.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:H/A:L).	5.9	More Details
CVE-2022-0023	An improper handling of exceptional conditions vulnerability exists in the DNS proxy feature of Palo Alto Networks PAN-OS software that enables a meddler-in-the-middle (MITM) to send specifically crafted traffic to the firewall that causes the service to restart unexpectedly. Repeated attempts to send this request result in denial-of-service to all PAN-OS services by restarting the device in maintenance mode. This issue does not impact Panorama appliances and Prisma Access customers. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.22; PAN-OS 9.0 versions earlier than PAN-OS 9.0.16; PAN-OS 9.1 versions earlier than PAN-OS 9.1.13; PAN-OS 10.0 versions earlier than PAN-OS 10.0.10; PAN-OS 10.1 versions earlier than PAN-OS 10.1.5. This issue does not impact PAN-OS 10.2.	5.9	More Details
CVE-2021-39072	IBM Security Guardium 11.3 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 215581.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21473	Vulnerability in the Oracle Banking Treasury Management product of Oracle Financial Services Applications (component: Infrastructure). The supported version that is affected is 14.5. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Treasury Management. 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 Banking Treasury Management accessible data as well as unauthorized read access to a subset of Oracle Banking Treasury Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Treasury Management. CVSS 3.1 Base Score 5.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:H/A:L).	5.9	More Details
CVE-2022-24825	Smokescreen is a simple HTTP proxy that fogs over naughty URLs. The primary use case for Smokescreen is to prevent server-side request forgery (SSRF) attacks in which external attackers leverage the behavior of applications to connect to or scan internal infrastructure. Smokescreen also offers an option to deny access to additional (e.g., external) URLs by way of a deny list. There was an issue in Smokescreen that made it possible to bypass the deny list feature by appending a dot to the end of user-supplied URLs, or by providing input in a different letter case. Recommended to upgrade Smokescreen to version 0.0.3 or later.	5.8	More Details
CVE-2021-23286	Eaton Intelligent Power Manager Infrastructure (IPM Infrastructure) version 1.5.0plus205 and all prior versions are vulnerable to CSV Formula Injection. This issue affects: Eaton Intelligent Power Manager Infrastructure (IPM Infrastructure) all version 1.5.0plus205 and prior versions.	5.7	More Details
CVE-2021-23284	Eaton Intelligent Power Manager Infrastructure (IPM Infrastructure) version 1.5.0plus205 and all prior versions are vulnerable to Stored Cross-site Scripting vulnerability. This issue affects: Eaton Intelligent Power Manager Infrastructure (IPM Infrastructure) all version 1.5.0plus205 and prior versions.	5.7	More Details
CVE-2022-1382	NULL Pointer Dereference in GitHub repository radareorg/radare2 prior to 5.6.8. This vulnerability is capable of making the radare2 crash, thus affecting the availability of the system.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21461	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Solaris accessible data. CVSS 3.1 Base Score 5.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	5.5	More Details
CVE-2022-21463	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. 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-2022-21425	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). 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 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-2022-22193	An Improper Handling of Unexpected Data Type vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). Continued execution of this command might cause a sustained Denial of Service condition. If BGP rib sharding is configured and a certain CLI command is executed the rpd process can crash. During the rpd crash and restart, the routing protocols might be impacted and traffic disruption might be seen due to the loss of routing information. This issue affects: Juniper Networks Junos OS 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2. Juniper Networks Junos OS Evolved 20.4 versions prior to 20.4R3-EVO; 21.1 versions prior to 21.1R3-EVO; 21.2 versions prior to 21.2R2-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 20.3R1. Juniper Networks Junos OS Evolved versions prior to 20.3R1-EVO.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24493	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability	5.5	More Details
CVE-2022-21459	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 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-2022-28966	Wasm3 0.5.0 has a heap-based buffer overflow in NewCodePage in m3_code.c (called indirectly from Compile_BranchTable in m3_compile.c).	5.5	More Details
CVE-2022-0221	A CWE-611: Improper Restriction of XML External Entity Reference vulnerability exists that could result in information disclosure when opening a malicious solution file provided by an attacker with SCADAPack Workbench. This could be exploited to pass data from local files to a remote system controlled by an attacker. Affected Product: SCADAPack Workbench (6.6.8a and prior)	5.5	More Details
CVE-2022-21478	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 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-2022-21479	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 and unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:H).	5.5	More Details
CVE-2022-21440	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 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-2022-21405	Vulnerability in the OSS Support Tools product of Oracle Support Tools (component: Oracle Explorer). The supported version that is affected is 18.3. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where OSS Support Tools executes to compromise OSS Support Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in OSS Support Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all OSS Support Tools accessible data. CVSS 3.1 Base Score 5.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:C/C:H/I:N/A:N).	5.5	More Details
CVE-2022-24548	Microsoft Defender Denial of Service Vulnerability	5.5	More Details
CVE-2022-26920	Windows Graphics Component Information Disclosure Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20724	Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software. For more information about these vulnerabilities, see the Details section of this advisory.	5.5	More Details
CVE-2021-3681	A flaw was found in Ansible Galaxy Collections. When collections are built manually, any files in the repository directory that are not explicitly excluded via the ``build_ignore`` list in "galaxy.yml" include files in the ``.tar.gz`` file. This contains sensitive info, such as the user's Ansible Galaxy API key and any secrets in ``ansible`` or ``ansible-playbook`` verbose output without the``no_log`` redaction. Currently, there is no way to deprecate a Collection Or delete a Collection Version. Once published, anyone who downloads or installs the collection can view the secrets.	5.5	More Details
CVE-2022-28049	NGINX NJS 0.7.2 was discovered to contain a NULL pointer dereference via the component njs_vmcode_array at /src/njs_vmcode.c.	5.5	More Details
CVE-2022-20677	Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software. For more information about these vulnerabilities, see the Details section of this advisory.	5.5	More Details
CVE-2022-20717	A vulnerability in the NETCONF process of Cisco SD-WAN vEdge Routers could allow an authenticated, local attacker to cause an affected device to run out of memory, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient memory management when an affected device receives large amounts of traffic. An attacker could exploit this vulnerability by sending malicious traffic to an affected device. A successful exploit could allow the attacker to cause the device to crash, resulting in a DoS condition.	5.5	More Details
CVE-2022-20718	Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software. For more information about these vulnerabilities, see the Details section of this advisory.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20719	Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software. For more information about these vulnerabilities, see the Details section of this advisory.	5.5	More Details
CVE-2022-24308	Automox Agent prior to version 37 on Windows and Linux and Version 36 on OSX could allow for a non privileged user to obtain sensitive information during the install process.	5.5	More Details
CVE-2022-20720	Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software. For more information about these vulnerabilities, see the Details section of this advisory.	5.5	More Details
CVE-2022-20722	Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software. For more information about these vulnerabilities, see the Details section of this advisory.	5.5	More Details
CVE-2022-20723	Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software. For more information about these vulnerabilities, see the Details section of this advisory.	5.5	More Details
CVE-2022-20721	Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software. For more information about these vulnerabilities, see the Details section of this advisory.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20726	Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software. For more information about these vulnerabilities, see the Details section of this advisory.	5.5	More Details
CVE-2022-24484	Windows Cluster Shared Volume (CSV) Denial of Service Vulnerability	5.5	More Details
CVE-2022-20727	Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software. For more information about these vulnerabilities, see the Details section of this advisory.	5.5	More Details
CVE-2011-4917	In the Linux kernel through 3.1 there is an information disclosure issue via /proc/stat.	5.5	More Details
CVE-2022-20725	Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software. For more information about these vulnerabilities, see the Details section of this advisory.	5.5	More Details
CVE-2020-13495	An exploitable vulnerability exists in the way Pixar OpenUSD 20.05 handles file offsets in binary USD files. A specially crafted malformed file can trigger an arbitrary out-of-bounds memory access that could lead to the disclosure of sensitive information. This vulnerability could be used to bypass mitigations and aid additional exploitation. To trigger this vulnerability, the victim needs to access an attacker-provided file.	5.5	More Details
CVE-2022-24483	Windows Kernel Information Disclosure Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21477	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Attachments, File Upload). Supported versions that are affected are 12.2.6-12.2.11. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Framework, 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 Applications Framework accessible data as well as unauthorized read access to a subset of Oracle Applications Framework 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-2022-1351	Stored XSS in Tooltip in GitHub repository pimcore/pimcore prior to 10.4.	5.4	More Details
CVE-2021-45227	An issue was discovered in COINS Construction Cloud 11.12. Due to an inappropriate use of HTML IFRAME elements, the file upload functionality is vulnerable to a persistent Cross-Site Scripting (XSS) attack.	5.4	More Details
CVE-2022-1380	Stored Cross Site Scripting vulnerability in Item name parameter in GitHub repository snipe/snipe-it prior to v5.4.3. The vulnerability is capable of stolen the user Cookie.	5.4	More Details
CVE-2021-43633	Sourcecodester Messaging Web Application 1.0 is vulnerable to stored XSS. If a sender inserts valid scripts into the chat, the script will be executed on the receiver chat.	5.4	More Details
CVE-2021-43288	An issue was discovered in ThoughtWorks GoCD before 21.3.0. An attacker in control of a GoCD Agent can plant malicious JavaScript into a failed Job Report.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21411	Vulnerability in the RDBMS Gateway / Generic ODBC Connectivity component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 19c and 21c. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise RDBMS Gateway / Generic ODBC Connectivity. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of RDBMS Gateway / Generic ODBC Connectivity accessible data as well as unauthorized read access to a subset of RDBMS Gateway / Generic ODBC Connectivity 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-2022-27851	Cross-Site Request Forgery (CSRF) in Use Any Font (WordPress plugin) <= 6.1.7 allows an attacker to deactivate the API key.	5.4	More Details
CVE-2022-27850	Cross-Site Request Forgery (CSRF) in Simple Ajax Chat (WordPress plugin) <= 20220115 allows an attacker to clear the chat log or delete a chat message.	5.4	More Details
CVE-2022-21481	Vulnerability in the PeopleSoft Enterprise FIN Cash Management product of Oracle PeopleSoft (component: Financial Gateway). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise FIN Cash Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise FIN Cash Management, 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 FIN Cash Management accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise FIN Cash Management 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-2022-21450	Vulnerability in the PeopleSoft Enterprise PRTL Interaction Hub product of Oracle PeopleSoft (component: My Links). The supported version that is affected is 9.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PRTL Interaction Hub. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PRTL Interaction Hub, 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 PRTL Interaction Hub accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PRTL Interaction Hub 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-2021-43742	CMSimple 5.4 is vulnerable to Cross Site Scripting (XSS) via the file upload feature.	5.4	More Details
CVE-2021-45228	An XSS issue was discovered in COINS Construction Cloud 11.12. Due to insufficient neutralization of user input in the description of a task, it is possible to store malicious JavaScript code in the task description. This is later executed when it is reflected back to the user.	5.4	More Details
CVE-2022-0765	The Loco Translate WordPress plugin before 2.6.1 does not properly remove inline events from elements in the source translation strings before outputting them in the editor in the plugin admin panel, allowing any user with access to the plugin (Translator and Administrator by default) to add arbitrary javascript payloads to the source strings leading to a stored cross-site scripting (XSS) vulnerability.	5.4	More Details
CVE-2021-41570	Veritas NetBackup OpsCenter Analytics 9.1 allows XSS via the NetBackup Master Server Name, Display Name, NetBackup User Name, or NetBackup Password field during a Settings/Configuration Add operation.	5.4	More Details
CVE-2022-1112	The Autolinks WordPress plugin through 1.0.1 does not have CSRF check in place when updating its settings, and does not sanitise as well as escape them, which could allow attackers to perform Stored Cross-Site scripting against a logged in admin via a CSRF attack	5.4	More Details
CVE-2022-26593	Cross-site scripting (XSS) vulnerability in the Asset module's asset categories selector in Liferay Portal 7.3.3 through 7.4.0, and Liferay DXP 7.3 before service pack 3 allows remote attackers to inject arbitrary web script or HTML via the name of a asset category.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25154	An open redirect vulnerability in the administrative interface of the B. Braun Melsungen AG SpaceCom device Version L81/U61 and earlier, and the Data module compactplus Versions A10 and A11 allows attackers to redirect users to malicious websites.	5.4	More Details
CVE-2022-26907	Azure SDK for .NET Information Disclosure Vulnerability	5.3	More Details
CVE-2022-24824	Discourse is an open source platform for community discussion. In affected versions an attacker can poison the cache for anonymous (i.e. not logged in) users, such that the users are shown the crawler view of the site instead of the HTML page. This can lead to a partial denial-of-service. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. There are no known workarounds for this issue.	5.3	More Details
CVE-2022-21426	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. 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 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. 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-2022-27863	Sensitive Information Exposure in E4J s.r.l. VikBooking Hotel Booking Engine & PMS plugin <= 1.5.3 on WordPress allows attackers to get the booking data by guessing / brute-forcing easy predictable booking IDs via search POST requests.	5.3	More Details
CVE-2022-22968	In Spring Framework versions 5.3.0 - 5.3.18, 5.2.0 - 5.2.20, and older unsupported versions, the patterns for disallowedFields on a DataBinder are case sensitive which means a field is not effectively protected unless it is listed with both upper and lower case for the first character of the field, including upper and lower case for the first character of all nested fields within the property path.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21434	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. 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-2022-27652	A flaw was found in cri-o, where containers were incorrectly started with non-empty default permissions. A vulnerability was found in Moby (Docker Engine) where containers started incorrectly with non-empty inheritable Linux process capabilities. This flaw allows an attacker with access to programs with inheritable file capabilities to elevate those capabilities to the permitted set when execve(2) runs.	5.3	More Details
CVE-2022-26910	Skype for Business and Lync Spoofing Vulnerability	5.3	More Details
CVE-2022-24850	Discourse is an open source platform for community discussion. A category's group permissions settings can be viewed by anyone that has access to the category. As a result, a normal user is able to see whether a group has read/write permissions in the category even though the information should only be available to the users that can manage a category. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. There are no workarounds for this problem.	5.3	More Details
CVE-2021-42782	Stack buffer overflow issues were found in Opensc before version 0.22.0 in various places that could potentially crash programs using the library.	5.3	More Details
CVE-2022-26643	An issue in EasyIO CPT Graphics v0.8 allows attackers to discover valid users in the application.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41119	Wire-server is the system server for the wire back-end services. Releases prior to v2022-03-01 are subject to a denial of service attack via a crafted object causing a hash collision. This collision causes the server to spend at least quadratic time parsing it which can lead to a denial of service for a heavily used server. The issue has been fixed in wire-server 2022-03-01 and is already deployed on all Wire managed services. On premise instances of wire-server need to be updated to 2022-03-01, so that their backends are no longer affected. There are no known workarounds for this issue.	5.3	More Details
CVE-2021-42781	Heap buffer overflow issues were found in Opensc before version 0.22.0 in pkcs15-oberthur.c that could potentially crash programs using the library.	5.3	More Details
CVE-2022-22961	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain an information disclosure vulnerability due to returning excess information. A malicious actor with remote access may leak the hostname of the target system. Successful exploitation of this issue can lead to targeting victims.	5.3	More Details
CVE-2022-27849	Sensitive Information Disclosure (sac-export.csv) in Simple Ajax Chat (WordPress plugin) <= 20220115	5.3	More Details
CVE-2021-42780	A use after return issue was found in Opensc before version 0.22.0 in insert_pin function that could potentially crash programs using the library.	5.3	More Details
CVE-2022-1054	The RSVP and Event Management Plugin WordPress plugin before 2.7.8 does not have any authorisation checks when exporting its entries, and has the export function hooked to the init action. As a result, unauthenticated attackers could call it and retrieve PII such as first name, last name and email address of user registered for events	5.3	More Details
CVE-2022-1186	The WordPress plugin Be POPIA Compliant exposed sensitive information to unauthenticated users consisting of site visitors emails and usernames via an API route, in versions up to an including 1.1.5.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21496	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JNDI). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. 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-2021-42779	A heap use after free issue was found in Opensc before version 0.22.0 in sc_file_valid.	5.3	More Details
CVE-2021-42778	A heap double free issue was found in Opensc before version 0.22.0 in sc_pkcs15_free_tokeninfo.	5.3	More Details
CVE-2022-26777	Zoho ManageEngine Remote Access Plus before 10.1.2137.15 allows guest users to view license details.	5.3	More Details
CVE-2022-26653	Zoho ManageEngine Remote Access Plus before 10.1.2137.15 allows guest users to view domain details (such as the username and GUID of an administrator).	5.3	More Details
CVE-2022-1019	Automated Logic's WebCtrl Server Version 6.1 'Help' index pages are vulnerable to open redirection. The vulnerability allows an attacker to send a maliciously crafted URL which could result in redirecting the user to a malicious webpage or downloading a malicious file.	5.2	More Details
CVE-2021-23283	Eaton Intelligent Power Protector (IPP) prior to version 1.69 is vulnerable to stored Cross Site Scripting. The vulnerability exists due to insufficient validation of user input and improper encoding of the output for certain resources within the IPP software.	5.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20676	A vulnerability in the Tool Command Language (Tcl) interpreter of Cisco IOS XE Software could allow an authenticated, local attacker to escalate from privilege level 15 to root-level privileges. This vulnerability is due to insufficient input validation of data that is passed into the Tcl interpreter. An attacker could exploit this vulnerability by loading malicious Tcl code on an affected device. A successful exploit could allow the attacker to execute arbitrary commands as root. By default, Tcl shell access requires privilege level 15.	5.1	More Details
CVE-2022-25166	An issue was discovered in Amazon AWS VPN Client 2.0.0. It is possible to include a UNC path in the OpenVPN configuration file when referencing file paths for parameters (such as auth-user-pass). When this file is imported and the client attempts to validate the file path, it performs an open operation on the path and leaks the user's Net-NTLMv2 hash to an external server. This could be exploited by having a user open a crafted malicious ovpn configuration file.	5.0	More Details
CVE-2022-21416	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Utility). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. 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 Solaris accessible data. CVSS 3.1 Base Score 5.0 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N).	5.0	More Details
CVE-2022-21418	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.28 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 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 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).	5.0	More Details
CVE-2022-29287	Kentico CMS before 13.0.66 has an Insecure Direct Object Reference vulnerability. It allows an attacker with user management rights (default is Administrator) to export the user options of any user, even ones with higher privileges (like Global Administrators) than the current user. The exported XML contains every option of the exported user (even the hashed password).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21412	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-2020-25167	OSIsoft PI Vision 2020 versions prior to 3.5.0 could disclose information to a user with insufficient privileges for an AF attribute.	4.9	More Details
CVE-2022-21462	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-2022-26897	Azure Site Recovery Information Disclosure Vulnerability	4.9	More Details
CVE-2022-22279	A post-authentication arbitrary file read vulnerability impacting end-of-life Secure Remote Access (SRA) products and older firmware versions of Secure Mobile Access (SMA) 100 series products, specifically the SRA appliances running all 8.x, 9.0.0.5-19sv and earlier versions and Secure Mobile Access (SMA) 100 series products running older firmware 9.0.0.9-26sv and earlier versions	4.9	More Details
CVE-2022-26896	Azure Site Recovery Information Disclosure Vulnerability	4.9	More Details
CVE-2022-21452	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 Number	Description	Base Score	Reference
CVE-2022-21427	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 5.7.37 and prior and 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-2022-21413	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). 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-2022-21414	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-2022-21417	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.37 and prior and 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 Number	Description	Base Score	Reference
CVE-2022-21415	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). 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-2022-21435	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-2022-21436	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-2022-21438	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-2022-21437	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 Number	Description	Base Score	Reference
CVE-2022-1088	The Page Security & Membership WordPress plugin through 1.5.15 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-1063	The Thank Me Later WordPress plugin through 3.3.4 does not sanitise and escape the Message Subject field before outputting it in the Messages list, which could allow high privileges users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-27853	Authenticated (author or higher role) Stored Cross-Site Scripting (XSS) in Contest Gallery (WordPress plugin) <= 13.1.0.9	4.8	More Details
CVE-2021-36828	Authenticated (admin+) Stored Cross-Site Scripting (XSS) in WP Maintenance plugin <= 6.0.7 versions.	4.8	More Details
CVE-2022-21145	A stored cross-site scripting vulnerability exists in the WebUserActions.aspx functionality of Lansweeper lansweeper 9.1.20.2. A specially-crafted HTTP request can lead to arbitrary Javascript code injection. An attacker can send an HTTP request to trigger this vulnerability.	4.8	More Details
CVE-2022-0706	The Easy Digital Downloads WordPress plugin before 2.11.6 does not sanitise and escape the Downloadable File Name in the Logs, which could allow high privilege users to perform Cross-Site Scripting attacks when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-1001	The WP Downgrade WordPress plugin before 1.2.3 only perform client side validation of its "WordPress Target Version" settings, but does not sanitise and escape it server side, allowing high privilege users such as admin to perform Cross-Site attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-1090	The Good & Bad Comments WordPress plugin through 1.0.0 does not sanitise and escape its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-0994	The Hummingbird WordPress plugin before 3.3.2 does not sanitise and escape the Config Name, which could allow high privilege users, such as admin to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0737	The Text Hover WordPress plugin before 4.2 does not sanitize and escape the text to hover, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2022-1384	Mattermost version 6.4.x and earlier fails to properly check the plugin version when a plugin is installed from the Marketplace, which allows an authenticated and an authorized user to install and exploit an old plugin version from the Marketplace which might have known vulnerabilities.	4.7	More Details
CVE-2022-21469	Vulnerability in the Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: UI Framework). Supported versions that are affected are 13.4.0.0 and 13.5.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Enterprise Manager Base Platform. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Enterprise Manager Base Platform, 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 Enterprise Manager Base Platform accessible data. CVSS 3.1 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	4.7	More Details
CVE-2022-20693	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to perform an injection attack against an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI API. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	4.7	More Details
CVE-2022-20731	Multiple vulnerabilities that affect Cisco Catalyst Digital Building Series Switches and Cisco Catalyst Micro Switches could allow an attacker to execute persistent code at boot time or to permanently prevent the device from booting, resulting in a permanent denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory.	4.6	More Details
CVE-2022-20661	Multiple vulnerabilities that affect Cisco Catalyst Digital Building Series Switches and Cisco Catalyst Micro Switches could allow an attacker to execute persistent code at boot time or to permanently prevent the device from booting, resulting in a permanent denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27817	SWHKD 1.1.5 consumes the keyboard events of unintended users. This could potentially cause an information leak, but is usually a denial of functionality.	4.4	More Details
CVE-2022-21460	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Logging). Supported versions that are affected are 5.7.37 and prior and 8.0.28 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 access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N).	4.4	More Details
CVE-2022-21451	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.37 and prior and 8.0.28 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 ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details
CVE-2022-21444	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 5.7.37 and prior and 8.0.28 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 ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details
CVE-2021-39078	IBM Security Guardium 10.5 stores user credentials in plain clear text which can be read by a local privileged user. IBM X-Force ID: 215589.	4.4	More Details
CVE-2022-1332	One of the API in Mattermost version 6.4.1 and earlier fails to properly protect the permissions, which allows the authenticated members with restricted custom admin role to bypass the restrictions and view the server logs and server config.json file contents.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27847	Cross-Site Request Forgery (CSRF) vulnerability in Yooslider Yoo Slider <= 2.0.0 on WordPress allows attackers to import templates.	4.3	More Details
CVE-2022-26595	Liferay Portal 7.3.7, 7.4.0, and 7.4.1, and Liferay DXP 7.2 fix pack 13, and 7.3 fix pack 2 does not properly check user permission when accessing a list of sites/groups, which allows remote authenticated users to view sites/groups via the user's site membership assignment UI.	4.3	More Details
CVE-2022-0707	The Easy Digital Downloads WordPress plugin before 2.11.6 does not have CSRF check in place when inserting payment notes, which could allow attackers to make a logged admin insert arbitrary notes via a CSRF attack	4.3	More Details
CVE-2022-1328	Buffer Overflow in uudecoder in Mutt affecting all versions starting from 0.94.13 before 2.2.3 allows read past end of input line	4.3	More Details
CVE-2022-1350	A vulnerability classified as problematic was found in GhostPCL 9.55.0. This vulnerability affects the function chunk_free_object of the file gsmchunk.c. The manipulation with a malicious file leads to a memory corruption. The attack can be initiated remotely but requires user interaction. The exploit has been disclosed to the public as a POC and may be used. It is recommended to apply the patches to fix this issue.	4.3	More Details
CVE-2022-28868	An Address bar spoofing vulnerability was discovered in Safe Browser for Android. When user clicks on a specially crafted malicious webpage/URL, user may be tricked for a short period of time (until the page loads) to think content may be coming from a valid domain, while the content comes from the attacker controlled site.	4.3	More Details
CVE-2022-28869	A vulnerability affecting F-Secure SAFE browser was discovered. A maliciously crafted website could make a phishing attack with address bar spoofing as the browser did not show full URL, such as port number.	4.3	More Details
CVE-2022-27846	Cross-Site Request Forgery (CSRF) vulnerability in Yooslider Yoo Slider <= 2.0.0 on WordPress allows attackers to create or modify slider.	4.3	More Details
CVE-2021-3503	A flaw was found in Wildfly where insufficient RBAC restrictions may lead to expose metrics data. The highest threat from this vulnerability is to the confidentiality.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22959	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a cross site request forgery vulnerability. A malicious actor can trick a user through a cross site request forgery to unintentionally validate a malicious JDBC URI.	4.3	More Details
CVE-2022-1337	The image proxy component in Mattermost version 6.4.1 and earlier allocates memory for multiple copies of a proxied image, which allows an authenticated attacker to crash the server via links to very large image files.	4.3	More Details
CVE-2022-28870	A vulnerability affecting F-Secure SAFE browser was discovered. A maliciously crafted website could make a phishing attack with address bar spoofing as the address bar was not correct if navigation fails.	4.3	More Details
CVE-2022-22391	IBM Aspera High-Speed Transfer 4.3.1 and earlier could allow an authenticated user to obtain information from non sensitive operating system files that they should not have access to. IBM X-Force ID: 222059.	4.3	More Details
CVE-2022-21494	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 4.0 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:N/I:N/A:H).	4.0	More Details
CVE-2022-21488	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.34. 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 update, insert or delete access to some of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.8 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:L/A:N).	3.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21487	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.34. 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-2022-1385	Mattermost 6.4.x and earlier fails to properly invalidate pending email invitations when the action is performed from the system console, which allows accidentally invited users to join the workspace and access information from the public teams and channels.	3.7	More Details
CVE-2022-21443	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. 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 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	3.7	More Details
CVE-2022-23292	Microsoft Power BI Spoofing Vulnerability	3.7	More Details
CVE-2022-1333	Mattermost Playbooks plugin v1.24.0 and earlier fails to properly check the limit on the number of webhooks, which allows authenticated and authorized users to create a specifically drafted Playbook which could trigger a large amount of webhook requests leading to Denial of Service.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27848	Authenticated (admin+ user) Stored Cross-Site Scripting (XSS) in Modern Events Calendar Lite (WordPress plugin) <= 6.5.1	3.4	More Details
CVE-2022-27814	SWHKD 1.1.5 allows arbitrary file-existence tests via the -c option.	3.3	More Details
CVE-2020-25168	Hard-coded credentials in the B. Braun Melsungen AG SpaceCom Version L81/U61 and earlier, and the Data module compactplus Versions A10 and A11 enable attackers with command line access to access the device's Wi-Fi module.	3.3	More Details
CVE-2021-23285	Eaton Intelligent Power Manager Infrastructure (IPM Infrastructure) version 1.5.0plus205 and all prior versions are vulnerable to reflected Cross-site Scripting vulnerability. This issue affects: Eaton Intelligent Power Manager Infrastructure (IPM Infrastructure) all version 1.5.0plus205 and prior versions.	3.1	More Details
CVE-2022-21486	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.35 and prior, 7.5.25 and prior, 7.6.21 and prior and 8.0.28 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 unauthorized read access to a subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L).	2.9	More Details
CVE-2022-21485	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.35 and prior, 7.5.25 and prior, 7.6.21 and prior and 8.0.28 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 unauthorized read access to a subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L).	2.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21484	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.35 and prior, 7.5.25 and prior, 7.6.21 and prior and 8.0.28 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 unauthorized read access to a subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L).	2.9	More Details
CVE-2022-21423	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). 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 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-2022-27506	Hard-coded credentials allow administrators to access the shell via the SD-WAN CLI	2.7	More Details
CVE-2022-29268	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2022-27458	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-27447. Reason: This candidate is a reservation duplicate of CVE-2022-27447. Notes: All CVE users should reference CVE-2022-27447 instead of this candidate.	N/A	More Details
CVE-2022-1246	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-1280. Reason: This candidate is a reservation duplicate of CVE-2022-1280. Notes: All CVE users should reference CVE-2022-1280 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-20324	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 Number	Description	Base Score	Reference
CVE-2022-27427	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-38745. Reason: This candidate is a duplicate of CVE-2021-38745. Notes: All CVE users should reference CVE-2021-38745 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details