SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 28 July 2021

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-2021-33032	A Remote Code Execution (RCE) vulnerability in the WebUI component of the eQ-3 HomeMatic CCU2 firmware up to and including version 2.57.5 and CCU3 firmware up to and including version 3.57.5 allows remote unauthenticated attackers to execute system commands as root via a simple HTTP request.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7388	Sage X3 Unauthenticated Remote Command Execution (RCE) as SYSTEM in AdxDSrv.exe component. By editing the client side authentication request, an attacker can bypass credential validation. While exploiting this does require knowledge of the installation path, that information can be learned by exploiting CVE-2020-7387. This issue was fixed in AdxAdmin 93.2.53, which ships with updates for on-premises versions of Sage X3 including Version 9 (components shipped with Syracuse 9.22.7.2 and later), Sage X3 HR & Payroll Version 9 (those components that ship with Syracuse 9.24.1.3), Version 11 (components shipped with Syracuse 11.25.2.6 and later), and Version 12 (components shipped with Syracuse 12.10.2.8 and later) of Sage X3. Other on-premises versions of Sage X3 are unsupported by the vendor.	10.0	More Details
CVE-2021-2447	Vulnerability in the Oracle Secure Global Desktop product of Oracle Virtualization (component: Server). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle Secure Global Desktop. While the vulnerability is in Oracle Secure Global Desktop, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Secure Global Desktop. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2021-25208	Arbitrary file upload vulnerability in SourceCodester Travel Management System v 1.0 allows attackers to execute arbitrary code via the file upload to updatepackage.php.	9.8	More Details
CVE-2021-25212	SQL injection vulnerability in SourceCodester Alumni Management System v 1.0 allows remote attackers to execute arbitrary SQL statements, via the id parameter to manage_event.php.	9.8	More Details
CVE-2021-26223	SQL injection vulnerability in SourceCodester CASAP Automated Enrollment System v 1.0 allows remote attackers to execute arbitrary SQL statements, via the id parameter to view_pay.php.	9.8	More Details
CVE-2021-25205	SQL injection vulnerability in SourceCodester E-Commerce Website V 1.0 allows remote attackers to execute arbitrary SQL statements, via the update parameter to empViewUpdate.php .	9.8	More Details
CVE-2021-25209	SQL injection vulnerability in SourceCodester Theme Park Ticketing System v 1.0 allows remote attackers to execute arbitrary SQL statements, via the id parameter to view_user.php .	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25211	Arbitrary file upload vulnerability in SourceCodester Ordering System v 1.0 allows attackers to execute arbitrary code, via the file upload to ordering\admin\products\edit.php.	9.8	More Details
CVE-2021-25213	SQL injection vulnerability in SourceCodester Travel Management System v 1.0 allows remote attackers to execute arbitrary SQL statements, via the catid parameter to subcat.php.	9.8	More Details
CVE-2021-24036	Passing an attacker controlled size when creating an IOBuf could cause integer overflow, leading to an out of bounds write on the heap with the possibility of remote code execution. This issue affects versions of folly prior to v2021.07.22.00. This issue affects HHVM versions prior to 4.80.5, all versions between 4.81.0 and 4.102.1, all versions between 4.103.0 and 4.113.0, and versions 4.114.0, 4.115.0, 4.116.0, 4.117.0, 4.118.0 and 4.118.1.	9.8	More Details
CVE-2020-14032	ASRock 4x4 BOX-R1000 before BIOS P1.40 allows privilege escalation via code execution in the SMM.	9.8	More Details
CVE-2021-25207	Arbitrary file upload vulnerability in SourceCodester E-Commerce Website v 1.0 allows attackers to execute arbitrary code via the file upload to prodViewUpdate.php.	9.8	More Details
CVE-2021-25203	Arbitrary file upload vulnerability in Victor CMS v 1.0 allows attackers to execute arbitrary code via the file upload to \CMSsite-master\admin\includes\admin_add_post.php.	9.8	More Details
CVE-2021-25206	Arbitrary file upload vulnerability in SourceCodester Responsive Ordering System v 1.0 allows attackers to execute arbitrary code via the file upload to Product_model.php.	9.8	More Details
CVE-2021-2456	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web General). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Business Intelligence Enterprise Edition. 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-2020-20741	Incorrect Access Control in Beckhoff Automation GmbH & Co. KG CX9020 with firmware version CX9020_CB3011_WEC7_HPS_v602_TC31_B4016.6 allows remote attackers to bypass authentication via the "CE Remote Display Tool" as it does not close the incoming connection on the Windows CE side if the credentials are incorrect.	9.8	More Details
CVE-2021-3169	An issue in Jumpserver before 2.6.2, before 2.5.4, before 2.4.5 allows attackers to create a connection token through an API which does not have access control and use it to access sensitive assets.	9.8	More Details
CVE-2021-37473	In NavigateCMS version 2.9.4 and below, function in `product.php` is vulnerable to sql injection on parameter `products-order` through a post request, which results in arbitrary sql query execution in the backend database.	9.8	More Details
CVE-2021-37475	In NavigateCMS version 2.9.4 and below, function in `templates.php` is vulnerable to sql injection on parameter `template-properties-order`, which results in arbitrary sql query execution in the backend database.	9.8	More Details
CVE-2021-37476	In NavigateCMS version 2.9.4 and below, function in `product.php` is vulnerable to sql injection on parameter `id` through a post request, which results in arbitrary sql query execution in the backend database.	9.8	More Details
CVE-2021-37477	In NavigateCMS version 2.9.4 and below, function in `structure.php` is vulnerable to sql injection on parameter `children_order`, which results in arbitrary sql query execution in the backend database.	9.8	More Details
CVE-2021-37478	In NavigateCMS version 2.9.4 and below, function `block` is vulnerable to sql injection on parameter `block-order`, which results in arbitrary sql query execution in the backend database.	9.8	More Details
CVE-2020-17952	A remote code execution (RCE) vulnerability in /library/think/App.php of Twothink v2.0 allows attackers to execute arbitrary PHP code.	9.8	More Details
CVE-2020-18170	An issue in the SeChangeNotifyPrivilege component of Abloy Key Manager Version 7.14301.0.0 allows attackers to escalate privileges via a change in permissions.	9.8	More Details
CVE-2020-18172	A code injection vulnerability in the SeDebugPrivilege component of Trezor Bridge 2.0.27 allows attackers to escalate privileges.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-18174	A process injection vulnerability in setup.exe of AutoHotkey 1.1.32.00 allows attackers to escalate privileges.	9.8	More Details
CVE-2021-37555	TX9 Automatic Food Dispenser v3.2.57 devices allow access to a shell as root/superuser, a related issue to CVE-2019-16734. To connect, the telnet service is used on port 23 with the default password of 059AnkJ for the root account. The user can then download the filesystem through preinstalled BusyBox utilities (e.g., tar and nc).	9.8	More Details
CVE-2021-25210	Arbitrary file upload vulnerability in SourceCodester Alumni Management System v 1.0 allows attackers to execute arbitrary code, via the file upload to manage_event.php.	9.8	More Details
CVE-2021-35464	ForgeRock AM server before 7.0 has a Java deserialization vulnerability in the jato.pageSession parameter on multiple pages. The exploitation does not require authentication, and remote code execution can be triggered by sending a single crafted /ccversion/* request to the server. The vulnerability exists due to the usage of Sun ONE Application Framework (JATO) found in versions of Java 8 or earlier	9.8	More Details
CVE-2021-37155	wolfSSL 4.6.x through 4.7.x before 4.8.0 does not produce a failure outcome when the serial number in an OCSP request differs from the serial number in the OCSP response.	9.8	More Details
CVE-2020-21937	An command injection vulnerability in HNAP1/SetWLanApcliSettings of Motorola CX2 router CX 1.0.2 Build 20190508 Rel.97360n allows attackers to execute arbitrary system commands.	9.8	More Details
CVE-2021-22727	A CWE-331: Insufficient Entropy vulnerability exists in EVlink City (EVC1S22P4 / EVC1S7P4 all versions prior to R8 V3.4.0.1), EVlink Parking (EVW2 / EVF2 / EV.2 all versions prior to R8 V3.4.0.1), and EVlink Smart Wallbox (EVB1A all versions prior to R8 V3.4.0.1) that could allow an attacker to gain unauthorized access to the charging station web server	9.8	More Details
CVE-2021-22729	A CWE-259: Use of Hard-coded Password vulnerability exists in EVlink City (EVC1S22P4 / EVC1S7P4 all versions prior to R8 V3.4.0.1), EVlink Parking (EVW2 / EVF2 / EV.2 all versions prior to R8 V3.4.0.1), and EVlink Smart Wallbox (EVB1A all versions prior to R8 V3.4.0.1) that could allow an attacker to gain unauthorized administrative privileges when accessing to the charging station web server.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22730	A CWE-798: Use of Hard-coded Credentials vulnerability exists in EVlink City (EVC1S22P4 / EVC1S7P4 all versions prior to R8 V3.4.0.1), EVlink Parking (EVW2 / EVF2 / EV.2 all versions prior to R8 V3.4.0.1), and EVlink Smart Wallbox (EVB1A all versions prior to R8 V3.4.0.1) that could an attacker to gain unauthorized administrative privileges when accessing to the charging station web server.	9.8	More Details
CVE-2021-22772	A CWE-306: Missing Authentication for Critical Function vulnerability exists in Easergy T200 ((Modbus) SC2-04MOD-07000100 and earlier), Easergy T200 ((IEC104) SC2-04IEC-07000100 and earlier), and Easergy T200 ((DNP3) SC2-04DNP-07000102 and earlier) that could cause unauthorized operation when authentication is bypassed.	9.8	More Details
CVE-2020-21935	A command injection vulnerability in HNAP1/GetNetworkTomographySettings of Motorola CX2 router CX 1.0.2 Build 20190508 Rel.97360n allows attackers to execute arbitrary code.	9.8	More Details
CVE-2021-2382	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Security). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 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 takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2021-2394	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 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 takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2021-2397	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 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 takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2463	Vulnerability in the Oracle Commerce Platform product of Oracle Commerce (component: Dynamo Application Framework). Supported versions that are affected are 11.0.0, 11.1.0, 11.2.0 and 11.3.0-11.3.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Platform. Successful attacks of this vulnerability can result in takeover of Oracle Commerce Platform. 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-2021-32744	Collabora Online is a collaborative online office suite. In versions prior to 4.2.17-1 and version 6.4.9-5, unauthenticated attackers are able to gain access to files which are currently opened by other users in the Collabora Online editor. For successful exploitation the attacker is required to guess the file identifier - the predictability of this file identifier is dependent on external file-storage implementations (this is a potential "IDOR" - Insecure Direct Object Reference - vulnerability). Versions 4.2.17-1 and 6.4.9-5 contain patches for this issue. There is no known workaround except updating the Collabora Online application to one of the patched releases.	9.8	More Details
CVE-2021-35522	A Buffer Overflow in Thrift command handlers in IDEMIA Morpho Wave Compact and VisionPass devices before 2.6.2, Sigma devices before 4.9.4, and MA VP MD devices before 4.9.7 allows remote attackers to achieve code execution, denial of services, and information disclosure via TCP/IP packets.	9.8	More Details
CVE-2019-20467	An issue was discovered on Sannce Smart HD Wifi Security Camera EAN 2 950004 595317 devices. The device by default has a TELNET interface available (which is not advertised or functionally used, but is nevertheless available). Two backdoor accounts (root and default) exist that can be used on this interface. The usernames and passwords of the backdoor accounts are the same on all devices. Attackers can use these backdoor accounts to obtain access and execute code as root within the device.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26765	SQL injection vulnerability in PHPGurukul Student Record System 4.0 allows remote attackers to execute arbitrary SQL statements, via the sid parameter to edit-sub.php.	9.8	More Details
CVE-2021-26228	SQL injection vulnerability in SourceCodester CASAP Automated Enrollment System v 1.0 allows remote attackers to execute arbitrary SQL statements, via the id parameter to edit_class1.php.	9.8	More Details
CVE-2021-26229	SQL injection vulnerability in SourceCodester CASAP Automated Enrollment System v 1.0 allows remote attackers to execute arbitrary SQL statements, via the id parameter to edit_stud.php.	9.8	More Details
CVE-2021-26231	SQL injection vulnerability in SourceCodester Fantastic Blog CMS v 1.0 allows remote attackers to execute arbitrary SQL statements, via the id parameter to category.php.	9.8	More Details
CVE-2021-26232	SQL injection vulnerability in SourceCodester Simple College Website v 1.0 allows remote attackers to execute arbitrary SQL statements via the id parameter to news.php.	9.8	More Details
CVE-2020-36033	SQL injection vulnerability in SourceCodester Water Billing System 1.0 via the id parameter to edituser.php.	9.8	More Details
CVE-2021-25202	SQL injection vulnerability in SourceCodester Sales and Inventory System v 1.0 allows remote attackers to execute arbitrary SQL statements, via the id parameter to \ahira\admin\inventory.php.	9.8	More Details
CVE-2021-26226	SQL injection vulnerability in SourceCodester CASAP Automated Enrollment System v 1.0 allows remote attackers to execute arbitrary SQL statements, via the id parameter to edit_user.php.	9.8	More Details
CVE-2021-22707	A CWE-798: Use of Hard-coded Credentials vulnerability exists in EVlink City (EVC1S22P4 / EVC1S7P4 all versions prior to R8 V3.4.0.1), EVlink Parking (EVW2 / EVF2 / EV.2 all versions prior to R8 V3.4.0.1), and EVlink Smart Wallbox (EVB1A all versions prior to R8 V3.4.0.1) that could allow an attacker to issue unauthorized commands to the charging station web server with administrative privileges.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2446	Vulnerability in the Oracle Secure Global Desktop product of Oracle Virtualization (component: Client). The supported version that is affected is 5.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Secure Global Desktop. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Secure Global Desktop, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Secure Global Desktop. CVSS 3.1 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).	9.6	More Details
CVE-2021-35942	The wordexp function in the GNU C Library (aka glibc) through 2.33 may crash or read arbitrary memory in parse_param (in posix/wordexp.c) when called with an untrusted, crafted pattern, potentially resulting in a denial of service or disclosure of information. This occurs because atoi was used but strtoul should have been used to ensure correct calculations.	9.1	More Details
CVE-2021-2355	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Marketing accessible data as well as unauthorized access to critical data or complete access to all Oracle Marketing accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	9.1	More Details
CVE-2021-20399	IBM Qradar SIEM 7.3.0 to 7.3.3 Patch 8 and 7.4.0 to 7.4.3 GA is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 196073.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference

CVE Number	Description	Base Score	Reference
CVE-2021-34619	The WooCommerce Stock Manager WordPress plugin is vulnerable to Cross-Site Request Forgery leading to Arbitrary File Upload in versions up to, and including, 2.5.7 due to missing nonce and file validation in the /woocommerce-stock-manager/trunk/admin/views/import-export.php file.	8.8	More Details
CVE-2015-2098	Multiple stack-based buffer overflows in WebGate eDVR Manager allow remote attackers to execute arbitrary code via unspecified vectors to the (1) Connect, (2) ConnectEx, or (3) ConnectEx2 function in the WESPEvent.WESPEventCtrl.1 control; (4) AudioOnlySiteChannel function in the WESPPlayback.WESPPlaybackCtrl.1 control; (5) Connect or (6) ConnectEx function in the WESPPTZ.WESPPTZCtrl.1 control; (7) SiteChannel property in the WESPPlayback.WESPPlaybackCtrl.1 control; (8) SiteName property in the WESPPlayback.WESPPlaybackCtrl.1 control; or (9) OpenDVrSSite function in the WESPPTZ.WESPPTZCtrl.1 control.	8.8	More Details
CVE-2021-37394	In RPCMS v1.8 and below, attackers can interact with API and change variable "role" to "admin" to achieve admin user registration.	8.8	More Details
CVE-2020-19498	Floating point exception in function Fraction in libheif 1.4.0, allows attackers to cause a Denial of Service or possibly other unspecified impacts.	8.8	More Details
CVE-2021-32756	ManageIQ is an open-source management platform. In versions prior to jansa-4, kasparov-2, and lasker-1, there is a flaw in the MiqExpression module of ManageIQ where a low privilege user could enter a crafted Ruby string which would be evaluated. Successful exploitation will allow an attacker to execute arbitrary code with root privileges on the host system. There are patches for this issue in releases named jansa-4, kasparov-2, and lasker-1. If possible, restrict users, via RBAC, to only the part of the application that they need access to. While MiqExpression is widely used throughout the product, restricting users can limit the surface of the attack.	8.8	More Details
CVE-2020-18171	TechSmith Snagit 19.1.0.2653 uses Object Linking and Embedding (OLE) which can allow attackers to obfuscate and embed crafted files used to escalate privileges. NOTE: This implies that Snagit's use of OLE is a security vulnerability unto itself and it is not. See reference document for more details	8.8	More Details
CVE-2021-37441	NCH Axon PBX v2.22 and earlier allows path traversal for file deletion via the logdelete?file=/.. substring.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2396	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: E-Business Suite - XDO). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in takeover of Oracle BI Publisher. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2020-19497	Integer overflow vulnerability in Mat_VarReadNextInfo5 in mat5.c in tbeu matio (aka MAT File I/O Library) 1.5.17, allows attackers to cause a Denial of Service or possibly other unspecified impacts.	8.8	More Details
CVE-2015-2100	Multiple stack-based buffer overflows in WebGate eDVR Manager and Control Center allow remote attackers to execute arbitrary code via unspecified vectors to the (1) TCPDiscover or (2) TCPDiscover2 function in the WESPDiscovery.WESPDiscoveryCtrl.1 control.	8.8	More Details
CVE-2015-2099	Multiple buffer overflows in WebGate Control Center allow remote attackers to execute arbitrary code via unspecified vectors to the (1) GetRecFileInfo function in the FileConverter.FileConverterCtrl.1 control, (2) Login function in the LoginContoller.LoginControllerCtrl.1 control, or (3) GetThumbnail function in the WESPPlayback.WESPPlaybackCtrl.1 control.	8.8	More Details
CVE-2021-30486	SysAid 20.3.64 b14 is affected by Blind and Stacker SQL injection via AssetManagementChart.jsp (GET computerID), AssetManagementChart.jsp (POST group1), AssetManagementList.jsp (GET computerID or group1), or AssetManagementSummary.jsp (GET group1).	8.8	More Details
CVE-2021-26764	SQL injection vulnerability in PHPGurukul Student Record System v 4.0 allows remote attackers to execute arbitrary SQL statements, via the id parameter to edit-std.php.	8.8	More Details
CVE-2021-26762	SQL injection vulnerability in PHPGurukul Student Record System 4.0 allows remote attackers to execute arbitrary SQL statements, via the cid parameter to edit-course.php.	8.8	More Details
CVE-2020-19499	An issue was discovered in heif::Box_iref::get_references in libheif 1.4.0, allows attackers to cause a Denial of Service or possibly other unspecified impact due to an invalid memory read.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2391	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Scheduler). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in takeover of Oracle BI Publisher. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2021-2392	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: BI Publisher Security). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in takeover of Oracle BI Publisher. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2021-37444	NCH IVM Attendant v5.12 and earlier suffers from a directory traversal weakness upon uploading plugins in a ZIP archive. This can lead to code execution if a ZIP element's pathname is set to a Windows startup folder, a file for the inbuilt Out-Going Message function, or a file for the the inbuilt Autodial function.	8.8	More Details
CVE-2021-31580	The restricted shell provided by Akkadian Provisioning Manager Engine (PME) can be bypassed by switching the OpenSSH channel from `shell` to `exec` and providing the ssh client a single execution parameter. This issue was resolved in Akkadian OVA appliance version 3.0 (and later), Akkadian Provisioning Manager 5.0.2 (and later), and Akkadian Appliance Manager 3.3.0.314-4a349e0 (and later).	8.7	More Details
CVE-2021-2349	Vulnerability in the Hyperion Essbase Administration Services product of Oracle Essbase (component: EAS Console). Supported versions that are affected are 11.1.2.4 and 21.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Hyperion Essbase Administration Services. While the vulnerability is in Hyperion Essbase Administration Services, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Hyperion Essbase Administration Services accessible data. CVSS 3.1 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32783	Contour is a Kubernetes ingress controller using Envoy proxy. In Contour before version 1.17.1 a specially crafted ExternalName type Service may be used to access Envoy's admin interface, which Contour normally prevents from access outside the Envoy container. This can be used to shut down Envoy remotely (a denial of service), or to expose the existence of any Secret that Envoy is using for its configuration, including most notably TLS Keypairs. However, it *cannot* be used to get the *content* of those secrets. Since this attack allows access to the administration interface, a variety of administration options are available, such as shutting down the Envoy or draining traffic. In general, the Envoy admin interface cannot easily be used for making changes to the cluster, in-flight requests, or backend services, but it could be used to shut down or drain Envoy, change traffic routing, or to retrieve secret metadata, as mentioned above. The issue will be addressed in Contour v1.18.0 and a cherry-picked patch release, v1.17.1, has been released to cover users who cannot upgrade at this time. For more details refer to the linked GitHub Security Advisory.	8.5	More Details
CVE-2021-1601	Multiple vulnerabilities in Cisco Intersight Virtual Appliance could allow an unauthenticated, adjacent attacker to access sensitive internal services from an external interface. These vulnerabilities are due to insufficient restrictions for IPv4 or IPv6 packets that are received on the external management interface. An attacker could exploit these vulnerabilities by sending specific traffic to this interface on an affected device. A successful exploit could allow the attacker to access sensitive internal services and make configuration changes on the affected device.	8.3	More Details
CVE-2021-1600	Multiple vulnerabilities in Cisco Intersight Virtual Appliance could allow an unauthenticated, adjacent attacker to access sensitive internal services from an external interface. These vulnerabilities are due to insufficient restrictions for IPv4 or IPv6 packets that are received on the external management interface. An attacker could exploit these vulnerabilities by sending specific traffic to this interface on an affected device. A successful exploit could allow the attacker to access sensitive internal services and make configuration changes on the affected device.	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2351	Vulnerability in the Advanced Networking Option component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Advanced Networking Option. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Advanced Networking Option, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Advanced Networking Option. Note: The July 2021 Critical Patch Update introduces a number of Native Network Encryption changes to deal with vulnerability CVE-2021-2351 and prevent the use of weaker ciphers. Customers should review: "Changes in Native Network Encryption with the July 2021 Critical Patch Update" (Doc ID 2791571.1). CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	8.3	More Details
CVE-2021-2409	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.24. 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. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details
CVE-2021-2436	Vulnerability in the Oracle Common Applications product of Oracle E-Business Suite (component: CRM User Management Framework). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Common Applications. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Applications, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Common Applications accessible data as well as unauthorized update, insert or delete access to some of Oracle Common Applications 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:R/S:C/C:H/I:L/A:N).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2359	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing 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:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2021-31579	Akkadian Provisioning Manager Engine (PME) ships with a hard-coded credential, akkadianuser:haakkadianpassword. This issue was resolved in Akkadian OVA appliance version 3.0 (and later), Akkadian Provisioning Manager 5.0.2 (and later), and Akkadian Appliance Manager 3.3.0.314-4a349e0 (and later).	8.2	More Details
CVE-2021-2405	Vulnerability in the Oracle Engineering product of Oracle E-Business Suite (component: Change Management). Supported versions that are affected are 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Engineering. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Engineering accessible data as well as unauthorized access to critical data or complete access to all Oracle Engineering accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2360	Vulnerability in the Oracle Approvals Management product of Oracle E-Business Suite (component: AME Page rendering). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Approvals Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Approvals Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Approvals Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2361	Vulnerability in the Oracle Advanced Inbound Telephony product of Oracle E-Business Suite (component: SDK client integration). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Advanced Inbound Telephony. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Advanced Inbound Telephony accessible data as well as unauthorized access to critical data or complete access to all Oracle Advanced Inbound Telephony accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2362	Vulnerability in the Oracle Field Service product of Oracle E-Business Suite (component: Wireless). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Field Service. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Field Service accessible data as well as unauthorized access to critical data or complete access to all Oracle Field Service accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2406	Vulnerability in the Oracle Collaborative Planning product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Collaborative Planning. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Collaborative Planning accessible data as well as unauthorized access to critical data or complete access to all Oracle Collaborative Planning accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-23412	All versions of package gitlogplus are vulnerable to Command Injection via the main functionality, as options attributes are appended to the command to be executed without sanitization.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2363	Vulnerability in the Oracle Public Sector Financials (International) product of Oracle E-Business Suite (component: Authorization). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Public Sector Financials (International). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Public Sector Financials (International) accessible data as well as unauthorized access to critical data or complete access to all Oracle Public Sector Financials (International) accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2364	Vulnerability in the Oracle iSupplier Portal product of Oracle E-Business Suite (component: Accounts). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle iSupplier Portal. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle iSupplier Portal accessible data as well as unauthorized access to critical data or complete access to all Oracle iSupplier Portal accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2415	Vulnerability in the Oracle Time and Labor product of Oracle E-Business Suite (component: Timecard). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Time and Labor. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Time and Labor accessible data as well as unauthorized access to critical data or complete access to all Oracle Time and Labor accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2365	Vulnerability in the Oracle Human Resources product of Oracle E-Business Suite (component: People Management). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Human Resources. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Human Resources accessible data as well as unauthorized access to critical data or complete access to all Oracle Human Resources accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2398	Vulnerability in the Oracle Advanced Outbound Telephony product of Oracle E-Business Suite (component: Region Mapping). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Advanced Outbound Telephony. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Advanced Outbound Telephony accessible data as well as unauthorized access to critical data or complete access to all Oracle Advanced Outbound Telephony accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2393	Vulnerability in the Oracle E-Records product of Oracle E-Business Suite (component: E-signatures). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle E-Records. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle E-Records accessible data as well as unauthorized access to critical data or complete access to all Oracle E-Records accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-37447	In NCH Quorum v2.03 and earlier, an authenticated user can use directory traversal via documentdelete?file=/.. for file deletion.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22726	A CWE-918: Server-Side Request Forgery (SSRF) vulnerability exists in EVlink City (EVC1S22P4 / EVC1S7P4 all versions prior to R8 V3.4.0.1), EVlink Parking (EVW2 / EVF2 / EV.2 all versions prior to R8 V3.4.0.1), and EVlink Smart Wallbox (EVB1A all versions prior to R8 V3.4.0.1) that could allow an attacker to perform unintended actions or access to data when crafted malicious parameters are submitted to the charging station web server.	8.1	More Details
CVE-2021-37443	NCH IVM Attendant v5.12 and earlier allows path traversal via the logdeleteselected check0 parameter for file deletion.	8.1	More Details
CVE-2021-2395	Vulnerability in the Oracle Hospitality Reporting and Analytics product of Oracle Food and Beverage Applications (component: iCare, Configuration). The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Reporting and Analytics. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized access to critical data or complete access to all Oracle Hospitality Reporting and Analytics accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2435	Vulnerability in the Essbase Analytic Provider Services product of Oracle Essbase (component: JAPI). The supported version that is affected is 11.1.2.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Essbase Analytic Provider Services. 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 Essbase Analytic Provider Services accessible data as well as unauthorized access to critical data or complete access to all Essbase Analytic Provider Services accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2434	Vulnerability in the Oracle Web Applications Desktop Integrator product of Oracle E-Business Suite (component: Application Service). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Web Applications Desktop Integrator. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Web Applications Desktop Integrator accessible data as well as unauthorized access to critical data or complete access to all Oracle Web Applications Desktop Integrator accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2428	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle Coherence. Successful attacks of this vulnerability can result in takeover of Oracle Coherence. 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-2021-21407	Combodo iTop is an open source, web based IT Service Management tool. Prior to version 2.7.4, the CSRF token validation can be bypassed through iTop portal via a tricky browser procedure. The vulnerability is patched in version 2.7.4 and 3.0.0.	8.0	More Details
CVE-2020-5370	Dell EMC OpenManage Enterprise (OME) versions prior to 3.4 contain an arbitrary file overwrite vulnerability. A remote authenticated malicious user with high privileges could potentially exploit this vulnerability to overwrite arbitrary files via directory traversal sequences using a crafted tar file to inject malicious RPMs which may cause a denial of service or perform unauthorized actions.	7.9	More Details
CVE-2021-31581	The restricted shell provided by Akkadian Provisioning Manager Engine (PME) can be escaped by abusing the 'Edit MySQL Configuration' command. This command launches a standard vi editor interface which can then be escaped. This issue was resolved in Akkadian OVA appliance version 3.0 (and later), Akkadian Provisioning Manager 5.0.2 (and later), and Akkadian Appliance Manager 3.3.0.314-4a349e0 (and later).	7.9	More Details
CVE-2020-18173	A DLL injection vulnerability in 1password.dll of 1Password 7.3.712 allows attackers to execute arbitrary code.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5316	Dell SupportAssist for Business PCs versions 2.0, 2.0.1, 2.0.2, 2.1, 2.1.1, 2.1.2, 2.1.3 and Dell SupportAssist for Home PCs version 2.0, 2.0.1, 2.0.2, 2.1, 2.1.1, 2.1.2, 2.1.3, 2.2, 2.2.1, 2.2.2, 2.2.3, 3.0, 3.0.1, 3.0.2, 3.1, 3.2, 3.2.1, 3.2.2, 3.3, 3.3.1, 3.3.2, 3.3.3, 3.4 contain an uncontrolled search path vulnerability. A locally authenticated low privileged user could exploit this vulnerability to cause the loading of arbitrary DLLs by the SupportAssist binaries, resulting in the privileged execution of arbitrary code.	7.8	More Details
CVE-2021-25808	A code injection vulnerability in backup/plugin.php of Bludit 3.13.1 allows attackers to execute arbitrary code via a crafted ZIP file.	7.8	More Details
CVE-2021-35482	An issue was discovered in Barco MirrorOp Windows Sender before 2.5.4.70. An attacker in the local network is able to achieve Remote Code Execution (with user privileges of the local user) on any device that tries to connect to a WePresent presentation system.	7.8	More Details
CVE-2021-1098	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it doesn't release some resources during driver unload requests from guests. This flaw allows a malicious guest to perform operations by reusing those resources, which may lead to information disclosure, data tampering, or denial of service. This affects vGPU version 12.x (prior to 12.3), version 11.x (prior to 11.5) and version 8.x (prior 8.8).	7.8	More Details
CVE-2021-1097	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it improperly validates the length field in a request from a guest. This flaw allows a malicious guest to send a length field that is inconsistent with the actual length of the input, which may lead to information disclosure, data tampering, or denial of service. This affects vGPU version 12.x (prior to 12.3), version 11.x (prior to 11.5) and version 8.x (prior 8.8).	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36934	An elevation of privilege vulnerability exists because of overly permissive Access Control Lists (ACLs) on multiple system files, including the Security Accounts Manager (SAM) database. An attacker who successfully exploited this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. An attacker must have the ability to execute code on a victim system to exploit this vulnerability. After installing this security update, you must manually delete all shadow copies of system files, including the SAM database, to fully mitigate this vulnerabilty. Simply installing this security update will not fully mitigate this vulnerability. See KB5005357- Delete Volume Shadow Copies.	7.8	More Details
CVE-2020-18169	A vulnerability in the Windows installer XML (WiX) toolset of TechSmith Snagit 19.1.1.2860 allows attackers to escalate privileges. NOTE: Exploit of the Snagit installer would require the end user to ignore other safety mechanisms provided by the Host OS. See reference document for more details	7.8	More Details
CVE-2021-1089	NVIDIA GPU Display Driver for Windows contains a vulnerability in nvidia-smi where an uncontrolled DLL loading path may lead to arbitrary code execution, denial of service, information disclosure, and data tampering.	7.8	More Details
CVE-2021-25698	The OpenSSL component of the Teradici PCoIP Standard Agent prior to version 21.07.0 was compiled without the no-autoload-config option, which allowed an attacker to elevate to the privileges of the running process via placing a specially crafted dll in a build configuration directory.	7.8	More Details
CVE-2020-19492	There is a floating point exception in ReadImage that leads to a Segmentation fault in sam2p 0.49.4. A crafted input will lead to a denial of service or possibly unspecified other impact.	7.8	More Details
CVE-2021-25699	The OpenSSL component of the Teradici PCoIP Software Client prior to version 21.07.0 was compiled without the no-autoload-config option, which allowed an attacker to elevate to the privileges of the running process via placing a specially crafted dll in a build configuration directory.	7.8	More Details
CVE-2020-19491	There is an invalid memory access bug in cgif.c that leads to a Segmentation fault in sam2p 0.49.4. A crafted input will lead to a denial of service or possibly unspecified other impact.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25695	The USB vHub in the Teradici PCOIP Software Agent prior to version 21.07.0 would accept commands from any program, which may allow an attacker to elevate privileges by changing the flow of program execution within the vHub driver.	7.8	More Details
CVE-2021-37576	arch/powerpc/kvm/book3s_rtas.c in the Linux kernel through 5.13.5 on the powerpc platform allows KVM guest OS users to cause host OS memory corruption via rtas_args.nargs, aka CID-f62f3c20647e.	7.8	More Details
CVE-2021-22777	A CWE-502: Deserialization of Untrusted Data vulnerability exists that could cause code execution by opening a malicious project file.	7.8	More Details
CVE-2021-32775	Combodo iTop is a web based IT Service Management tool. In versions prior to 2.7.4, a non admin user can get access to many class/field values through GroupBy Dashlet error message. This issue is fixed in versions 2.7.4 and 3.0.0.	7.7	More Details
CVE-2021-2458	Vulnerability in the Identity Manager product of Oracle Fusion Middleware (component: Identity Console). Supported versions that are affected are 11.1.2.2.0, 11.1.2.3.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Identity Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Identity Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Identity Manager accessible data as well as unauthorized update, insert or delete access to some of Identity Manager accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).	7.6	More Details
CVE-2021-2380	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Attachments / File Upload). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. 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. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Applications Framework accessible data as well as unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22523	XML External Entity vulnerability in Micro Focus Verastream Host Integrator, affecting version 7.8 Update 1 and earlier versions. The vulnerability could allow the control of web browser and hijacking user sessions.	7.6	More Details
CVE-2021-25201	SQL injection vulnerability in Learning Management System v 1.0 allows remote attackers to execute arbitrary SQL statements through the id parameter to obtain sensitive database information.	7.5	More Details
CVE-2021-2449	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. 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 Number	Description	Base Score	Reference
CVE-2021-2371	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 3.7.1.0, 12.1.3.0.0, 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 Coherence. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Coherence. 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-2021-2452	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. 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-2021-2451	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. 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 Number	Description	Base Score	Reference
CVE-2021-2420	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. 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-2021-2376	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 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-2021-22774	A CWE-759: Use of a One-Way Hash without a Salt vulnerability exists in EVlink City (EVC1S22P4 / EVC1S7P4 all versions prior to R8 V3.4.0.1), EVlink Parking (EVW2 / EVF2 / EV.2 all versions prior to R8 V3.4.0.1), and EVlink Smart Wallbox (EVB1A all versions prior to R8 V3.4.0.1) that could lead an attacker to get knowledge of charging station user account credentials using dictionary attacks techniques.	7.5	More Details
CVE-2021-2378	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 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 Number	Description	Base Score	Reference
CVE-2021-22146	All versions of Elastic Cloud Enterprise has the Elasticsearch “anonymous” user enabled by default in deployed clusters. While in the default setting the anonymous user has no permissions and is unable to successfully query any Elasticsearch APIs, an attacker could leverage the anonymous user to gain insight into certain details of a deployed cluster.	7.5	More Details
CVE-2021-2450	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. 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-2021-30110	dttray.exe in Greyware Automation Products Inc Domain Time II before 5.2.b.20210331 allows remote attackers to execute arbitrary code via a URL to a malicious update in a spoofed response to the UDP query used to check for updates.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28131	Impala sessions use a 16 byte secret to verify that the session is not being hijacked by another user. However, these secrets appear in the Impala logs, therefore Impala users with access to the logs can use another authenticated user's sessions with specially constructed requests. This means the attacker is able to execute statements for which they don't have the necessary privileges otherwise. Impala deployments with Apache Sentry or Apache Ranger authorization enabled may be vulnerable to privilege escalation if an authenticated attacker is able to hijack a session or query from another authenticated user with privileges not assigned to the attacker. Impala deployments with audit logging enabled may be vulnerable to incorrect audit logging as a user could undertake actions that were logged under the name of a different authenticated user. Constructing an attack requires a high degree of technical sophistication and access to the Impala system as an authenticated user. Mitigation: If an Impala deployment uses Apache Sentry, Apache Ranger or audit logging, then users should upgrade to a version of Impala with the fix for IMPALA-10600. The Impala 4.0 release includes this fix. This hides session secrets from the logs to eliminate the risk of any attack using this mechanism. In lieu of an upgrade, restricting access to logs that expose secrets will reduce the risk of an attack. Restricting access to the Impala deployment to trusted users will also reduce the risk of an attack. Log redaction techniques can be used to redact secrets from the logs.	7.5	More Details
CVE-2021-2400	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: E-Business Suite - XDO). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 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 BI Publisher. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle BI Publisher 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-2020-18428	tinyexr commit 0.9.5 was discovered to contain an array index error in the tinyexr::SaveEXR component, which can lead to a denial of service (DOS).	7.5	More Details
CVE-2020-18430	tinyexr 0.9.5 was discovered to contain an array index error in the tinyexr::DecodeEXRImage component, which can lead to a denial of service (DOS).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2388	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 8u291, 11.0.11, 16.0.1; Oracle GraalVM Enterprise Edition: 20.3.2 and 21.1.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).	7.5	More Details
CVE-2021-22001	In UAA versions prior to 75.3.0, sensitive information like relaying secret of the provider was revealed in response when deletion request of an identity provider(IdP) of type “oauth 1.0” was sent to UAA server.	7.5	More Details
CVE-2021-2423	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. 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-2021-33900	While investigating DIRSTUDIO-1219 it was noticed that configured StartTLS encryption was not applied when any SASL authentication mechanism (DIGEST-MD5, GSSAPI) was used. While investigating DIRSTUDIO-1220 it was noticed that any configured SASL confidentiality layer was not applied. This issue affects Apache Directory Studio version 2.0.0.v20210213-M16 and prior versions.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12681	Missing TLS certificate validation on 3xLogic Infinias eIDC32 devices through 3.4.125 allows an attacker to intercept/control the channel by which door lock policies are applied.	7.5	More Details
CVE-2021-34432	In Eclipse Mosquitto versions 2.07 and earlier, the server will crash if the client tries to send a PUBLISH packet with topic length = 0.	7.5	More Details
CVE-2021-2453	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. 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-2021-2430	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. 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-2021-35063	Suricata before 5.0.7 and 6.x before 6.0.3 has a "critical evasion."	7.5	More Details
CVE-2020-21933	An issue was discovered in Motorola CX2 router CX 1.0.2 Build 20190508 Rel.97360n where the admin password and private key could be found in the log tar package.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20596	NULL Pointer Dereference in MELSEC-F Series FX3U-ENET firmware version 1.14 and prior, FX3U-ENET-L firmware version 1.14 and prior and FX3U-ENET-P502 firmware version 1.14 and prior allows a remote unauthenticated attacker to cause a DoS condition in communication by sending specially crafted packets. Control by MELSEC-F series PLC is not affected and system reset is required for recovery.	7.5	More Details
CVE-2021-2431	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. 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-2021-32789	woocommerce-gutenberg-products-block is a feature plugin for WooCommerce Gutenberg Blocks. An SQL injection vulnerability impacts all WooCommerce sites running the WooCommerce Blocks feature plugin between version 2.5.0 and prior to version 2.5.16. Via a carefully crafted URL, an exploit can be executed against the `wc/store/products/collection-data?calculate_attribute_counts[][taxonomy]` endpoint that allows the execution of a read only sql query. There are patches for many versions of this package, starting with version 2.5.16. There are no known workarounds aside from upgrading.	7.5	More Details
CVE-2021-2350	Vulnerability in the Hyperion Essbase Administration Services product of Oracle Essbase (component: EAS Console). Supported versions that are affected are 11.1.2.4 and 21.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Hyperion Essbase Administration Services. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Hyperion Essbase Administration Services 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 Number	Description	Base Score	Reference
CVE-2021-2433	Vulnerability in the Essbase Analytic Provider Services product of Oracle Essbase (component: Web Services). Supported versions that are affected are 11.1.2.4 and 21.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Essbase Analytic Provider Services. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Essbase Analytic Provider Services. 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-2020-22284	A buffer overflow vulnerability in the zepif_linkoutput() function of Free Software Foundation lwIP git head version and version 2.1.2 allows attackers to access sensitive information via a crafted 6LoWPAN packet.	7.5	More Details
CVE-2020-22283	A buffer overflow vulnerability in the icmp6_send_response_with_addrs_and_netif() function of Free Software Foundation lwIP version git head allows attackers to access sensitive information via a crafted ICMPv6 packet.	7.5	More Details
CVE-2021-2344	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 3.7.1.0, 12.1.3.0.0, 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 Coherence. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Coherence. 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-2021-32761	Redis is an in-memory database that persists on disk. A vulnerability involving out-of-bounds read and integer overflow to buffer overflow exists starting with version 2.2 and prior to versions 5.0.13, 6.0.15, and 6.2.5. On 32-bit systems, Redis `*BIT*` command are vulnerable to integer overflow that can potentially be exploited to corrupt the heap, leak arbitrary heap contents or trigger remote code execution. The vulnerability involves changing the default `proto-max-bulk-len` configuration parameter to a very large value and constructing specially crafted commands bit commands. This problem only affects Redis on 32-bit platforms, or compiled as a 32-bit binary. Redis versions 5.0.`3m 6.0.15, and 6.2.5 contain patches for this issue. An additional workaround to mitigate the problem without patching the `redis-server` executable is to prevent users from modifying the `proto-max-bulk-len` configuration parameter. This can be done using ACL to restrict unprivileged users from using the CONFIG SET command.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23409	The package github.com/pires/go-proxyproto before 0.6.0 are vulnerable to Denial of Service (DoS) via creating connections without the proxy protocol header.	7.5	More Details
CVE-2021-36222	ec_verify in kdc/kdc_preauth_ec.c in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) before 1.18.4 and 1.19.x before 1.19.2 allows remote attackers to cause a NULL pointer dereference and daemon crash. This occurs because a return value is not properly managed in a certain situation.	7.5	More Details
CVE-2021-25804	A NULL-pointer dereference in "Open" in avi.c of VideoLAN VLC Media Player 3.0.11 can a denial of service (DOS) in the application.	7.5	More Details
CVE-2021-31292	An integer overflow in CrwMap::encode0x1810 of Exiv2 0.27.3 allows attackers to trigger a heap-based buffer overflow and cause a denial of service (DOS) via crafted metadata.	7.5	More Details
CVE-2020-21934	An issue was discovered in Motorola CX2 router CX 1.0.2 Build 20190508 Rel.97360n where authentication to download the Syslog could be bypassed.	7.5	More Details
CVE-2021-3663	firefly-iii is vulnerable to Improper Restriction of Excessive Authentication Attempts	7.5	More Details
CVE-2021-33629	isula-build before 0.9.5-6 can cause a program crash, when building container images, some functions for processing external data do not remove spaces when processing data.	7.5	More Details
CVE-2020-23282	SQL injection in Logon Page in MV's mConnect application, v02.001.00, allows an attacker to use a non existing user with a generic password to connect to the application and get access to unauthorized information.	7.5	More Details
CVE-2020-23283	Information disclosure in Logon Page in MV's mConnect application v02.001.00 allows an attacker to know valid users from the application's database via brute force.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2419	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. 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-2021-20337	IBM QRadar SIEM 7.3.0 to 7.3.3 Patch 8 and 7.4.0 to 7.4.3 GA uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 194448.	7.5	More Details
CVE-2021-29657	arch/x86/kvm/svm/nested.c in the Linux kernel before 5.11.12 has a use-after-free in which an AMD KVM guest can bypass access control on host OS MSRs when there are nested guests, aka CID-a58d9166a756. This occurs because of a TOCTOU race condition associated with a VMCB12 double fetch in nested_svm_vmrun.	7.4	More Details
CVE-2021-32745	Collabora Online is a collaborative online office suite. A reflected XSS vulnerability was found in Collabora Online prior to version 6.4.9-5. An attacker could inject unescaped HTML into a variable as they created the Collabora Online iframe, and execute scripts inside the context of the Collabora Online iframe. This would give access to a small set of user settings stored in the browser, as well as the session's authentication token which was also passed in at iframe creation time. The issue is patched in Collabora Online 6.4.9-5. Collabora Online 4.2 is not affected.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2443	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.24. 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. 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 and unauthorized read access to a subset of Oracle VM VirtualBox accessible data. Note: This vulnerability applies to Solaris x86 and Linux systems only. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:H).	7.3	More Details
CVE-2021-22771	A CWE-1236: Improper Neutralization of Formula Elements in a CSV File vulnerability exists in Easergy T300 with firmware V2.7.1 and older that would allow arbitrary command execution.	7.3	More Details
CVE-2021-29143	A remote execution of arbitrary commands vulnerability was discovered in Aruba CX 6200F Switch Series, Aruba 6300 Switch Series, Aruba 6400 Switch Series, Aruba 8320 Switch Series, Aruba 8325 Switch Series, Aruba 8400 Switch Series, Aruba CX 8360 Switch Series version(s): Aruba AOS-CX firmware: 10.04.xxxx - versions prior to 10.04.3070, 10.05.xxxx - versions prior to 10.05.0070, 10.06.xxxx - versions prior to 10.06.0110, 10.07.xxxx - versions prior to 10.07.0001. Aruba has released upgrades for Aruba AOS-CX devices that address this security vulnerability.	7.2	More Details
CVE-2021-34816	An Argument Injection issue in the plugin management of Etherpad 1.8.13 allows privileged users to execute arbitrary code on the server by installing plugins from an attacker-controlled source.	7.2	More Details
CVE-2021-2337	Vulnerability in the Oracle XML DB component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Any Procedure, Create Public Synonym privilege with network access via Oracle Net to compromise Oracle XML DB. Successful attacks of this vulnerability can result in takeover of Oracle XML DB. 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 Number	Description	Base Score	Reference
CVE-2021-22708	A CWE-347: Improper Verification of Cryptographic Signature vulnerability exists in EVlink City (EVC1S22P4 / EVC1S7P4 all versions prior to R8 V3.4.0.1), EVlink Parking (EVW2 / EVF2 / EV.2 all versions prior to R8 V3.4.0.1), and EVlink Smart Wallbox (EVB1A all versions prior to R8 V3.4.0.1) that could allow an attacker to craft a malicious firmware package and bypass the signature verification mechanism.	7.2	More Details
CVE-2021-2329	Vulnerability in the Oracle XML DB component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Any Procedure, Create Public Synonym privilege with network access via Oracle Net to compromise Oracle XML DB. Successful attacks of this vulnerability can result in takeover of Oracle XML DB. 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-2021-2328	Vulnerability in the Oracle Text component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Any Procedure, Alter Any Table privilege with network access via Oracle Net to compromise Oracle Text. Successful attacks of this vulnerability can result in takeover of Oracle Text. 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-2021-22522	Reflected Cross-Site Scripting vulnerability in Micro Focus Verastream Host Integrator, affecting version version 7.8 Update 1 and earlier versions. The vulnerability could allow disclosure of confidential data.	7.1	More Details
CVE-2021-25802	A buffer overflow vulnerability in the AVI_ExtractSubtitle component of VideoLAN VLC Media Player 3.0.11 allows attackers to cause an out-of-bounds read via a crafted .avi file.	7.1	More Details
CVE-2021-25801	A buffer overflow vulnerability in the __Parse_indx component of VideoLAN VLC Media Player 3.0.11 allows attackers to cause an out-of-bounds read via a crafted .avi file.	7.1	More Details
CVE-2021-26824	DM FingerTool v1.19 in the DM PD065 Secure USB is susceptible to improper authentication by a replay attack, allowing local attackers to bypass user authentication and access all features and data on the USB.	7.1	More Details
CVE-2021-1092	NVIDIA GPU Display Driver for Windows contains a vulnerability in the NVIDIA Control Panel application where it is susceptible to a Windows file system symbolic link attack where an unprivileged attacker can cause the applications to overwrite privileged files, resulting in potential denial of service or data loss.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1091	NVIDIA GPU Display driver for Windows contains a vulnerability where an unprivileged user can create a file hard link that causes the driver to overwrite a file that requires elevated privilege to modify, which could lead to data loss or denial of service.	7.1	More Details
CVE-2021-1090	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for control calls where the software reads or writes to a buffer by using an index or pointer that references a memory location after the end of the buffer, which may lead to data tampering or denial of service.	7.1	More Details
CVE-2021-25803	A buffer overflow vulnerability in the vlc_input_attachment_New component of VideoLAN VLC Media Player 3.0.11 allows attackers to cause an out-of-bounds read via a crafted .avi file.	7.1	More Details
CVE-2021-1099	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin) that could allow an attacker to cause stack-based buffer overflow and put a customized ROP gadget on the stack. Such an attack may lead to information disclosure, data tampering, or denial of service. This affects vGPU version 12.x (prior to 12.3), version 11.x (prior to 11.5) and version 8.x (prior 8.8).	7.0	More Details
CVE-2021-2454	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.24. Difficult to exploit 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. CVSS 3.1 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	7.0	More Details
CVE-2021-32794	ArchiSteamFarm is a C# application with primary purpose of idling Steam cards from multiple accounts simultaneously. Due to a bug in ASF code `POST /Api/ASF` ASF API endpoint responsible for updating global ASF config incorrectly removed `IPCPassword` from the resulting config when the caller did not specify it explicitly. Due to the above, it was possible for the user to accidentally remove `IPCPassword` security measure from his IPC interface when updating global ASF config, which exists as part of global config update functionality in ASF-ui. Removal of `IPCPassword` possesses a security risk, as unauthorized users may in result access the IPC interface after such modification. The issue is patched in ASF V5.1.2.4 and future versions. We recommend to manually verify that `IPCPassword` is specified after update, and if not, set it accordingly. In default settings, ASF is configured to allow IPC access from `localhost` only and should not affect majority of users.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32776	Combodo iTop is a web based IT Service Management tool. In versions prior to 2.7.4, CSRF tokens can be reused by a malicious user, as on Windows servers no cleanup is done on CSRF tokens. This issue is fixed in versions 2.7.4 and 3.0.0.	6.8	More Details
CVE-2021-33478	The TrustZone implementation in certain Broadcom MediaxChange firmware could allow an unauthenticated, physically proximate attacker to achieve arbitrary code execution in the TrustZone Trusted Execution Environment (TEE) of an affected device. This, for example, affects certain Cisco IP Phone and Wireless IP Phone products before 2021-07-07. Exploitation is possible only when the attacker can disassemble the device in order to control the voltage/current for chip pins.	6.8	More Details
CVE-2021-34259	A buffer overflow vulnerability in the USBH_ParseCfgDesc() function of STMicroelectronics STM32Cube Middleware v1.8.0 and below allows attackers to execute arbitrary code.	6.8	More Details
CVE-2021-34260	A buffer overflow vulnerability in the USBH_ParseInterfaceDesc() function of STMicroelectronics STM32Cube Middleware v1.8.0 and below allows attackers to execute arbitrary code.	6.8	More Details
CVE-2021-34262	A buffer overflow vulnerability in the USBH_ParseEPDesc() function of STMicroelectronics STM32Cube Middleware v1.8.0 and below allows attackers to execute arbitrary code.	6.8	More Details
CVE-2021-34431	In Eclipse Mosquitto version 1.6 to 2.0.10, if an authenticated client that had connected with MQTT v5 sent a crafted CONNECT message to the broker a memory leak would occur, which could be used to provide a DoS attack against the broker.	6.5	More Details
CVE-2021-37469	In NCH WebDictate v2.13 and earlier, authenticated users can abuse logprop?file=/.. path traversal to read files on the filesystem.	6.5	More Details
CVE-2021-1617	Multiple vulnerabilities in the web-based management interface of Cisco Intersight Virtual Appliance could allow an authenticated, remote attacker to conduct a path traversal or command injection attack on an affected system. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by using the web-based management interface to do one or both of the following: Execute a command using crafted input Upload a file that has been altered using path traversal techniques A successful exploit could allow the attacker to read and write arbitrary files or execute arbitrary commands as root on an affected system. For more information about these vulnerabilities, see the Details section of this advisory.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1618	Multiple vulnerabilities in the web-based management interface of Cisco Intersight Virtual Appliance could allow an authenticated, remote attacker to conduct a path traversal or command injection attack on an affected system. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by using the web-based management interface to do one or both of the following: Execute a command using crafted input Upload a file that has been altered using path traversal techniques A successful exploit could allow the attacker to read and write arbitrary files or execute arbitrary commands as root on an affected system. For more information about these vulnerabilities, see the Details section of this advisory.	6.5	More Details
CVE-2021-32795	ArchiSteamFarm is a C# application with primary purpose of idling Steam cards from multiple accounts simultaneously. In versions prior to 4.3.1.0 a Denial of Service (aka DoS) vulnerability which allows attacker to remotely crash running ASF instance through sending a specifically-crafted Steam chat message exists. The user sending the message does not need to be authorized within the bot or ASF process. The attacker needs to know ASF's `CommandPrefix` in advance, but majority of ASF setups run with an unchanged default value. This attack does not allow attacker to gain any potentially-sensitive information, such as logins or passwords, does not allow to execute arbitrary commands and otherwise exploit the crash further. The issue is patched in ASF V4.3.1.0. The only workaround which guarantees complete protection is running all bots with `OnlineStatus` of `0` (Offline). In this setup, ASF is able to ignore even the specifically-crafted message without attempting to interpret it.	6.5	More Details
CVE-2021-3198	By abusing the 'install rpm url' command, an attacker can escape the restricted clish shell on affected versions of Ivanti MobileIron Core. This issue was fixed in version 11.1.0.0.	6.5	More Details
CVE-2021-32631	Common is a package of common modules that can be accessed by NIMBLE services. Common before commit number 3b96cb0293d3443b870351945f41d7d55cb34b53 did not properly verify the signature of JSON Web Tokens. This allows someone to forge a valid JWT. Being able to forge JWTs may lead to authentication bypasses. Commit number 3b96cb0293d3443b870351945f41d7d55cb34b53 contains a patch for the issue. As a workaround, one may use the parseClaimsJws method to correctly verify the signature of a JWT.	6.5	More Details
CVE-2021-37445	In NCH Quorum v2.03 and earlier, an authenticated user can use directory traversal via logprop?file=/.. for file reading.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37439	NCH FlexiServer v6.00 suffers from a syslog?file=/.. path traversal vulnerability.	6.5	More Details
CVE-2021-29770	IBM i2 Analyst's Notebook Premium (IBM i2 Analyze 4.3.0, 4.3.1, and 4.3.2) could allow an authenticated user to perform unauthorized actions due to hazardous input validation. IBM X-Force ID: 202771.	6.5	More Details
CVE-2021-22144	In Elasticsearch versions before 7.13.3 and 6.8.17 an uncontrolled recursion vulnerability that could lead to a denial of service attack was identified in the Elasticsearch Grok parser. A user with the ability to submit arbitrary queries to Elasticsearch could create a malicious Grok query that will crash the Elasticsearch node.	6.5	More Details
CVE-2021-37440	NCH Axon PBX v2.22 and earlier allows path traversal for file disclosure via the logprop?file=/.. substring.	6.5	More Details
CVE-2021-20431	IBM i2 Analyst's Notebook Premium 9.2.0, 9.2.1, and 9.2.2 does not invalidate session after logout which could allow an an attacker to obtain sensitive information from the system. IBM X-Force ID: 196342.	6.5	More Details
CVE-2021-37442	NCH IVM Attendant v5.12 and earlier allows path traversal via viewfile?file=/.. to read files.	6.5	More Details
CVE-2020-4623	IBM i2 iBase 8.9.13 could allow a local authenticated attacker to execute arbitrary code on the system, caused by a DLL search order hijacking flaw. By using a specially-crafted .DLL file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 184984.	6.5	More Details
CVE-2021-36092	It's possible to create an email which contains specially crafted link and it can be used to perform XSS attack. This issue affects: OTRS AG ((OTRS)) Community Edition:6.0.x version 6.0.1 and later versions. OTRS AG OTRS: 7.0.x version 7.0.27 and prior versions; 8.0.x version 8.0.14 and prior versions.	6.5	More Details
CVE-2021-3540	By abusing the 'install rpm info detail' command, an attacker can escape the restricted clish shell on affected versions of Ivanti MobileIron Core. This issue was fixed in version 11.1.0.0.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32796	xmldom is an open source pure JavaScript W3C standard-based (XML DOM Level 2 Core) DOMParser and XMLSerializer module. xmldom versions 0.6.0 and older do not correctly escape special characters when serializing elements removed from their ancestor. This may lead to unexpected syntactic changes during XML processing in some downstream applications. This issue has been resolved in version 0.7.0. As a workaround downstream applications can validate the input and reject the maliciously crafted documents.	6.5	More Details
CVE-2021-22145	A memory disclosure vulnerability was identified in Elasticsearch 7.10.0 to 7.13.3 error reporting. A user with the ability to submit arbitrary queries to Elasticsearch could submit a malformed query that would result in an error message returned containing previously used portions of a data buffer. This buffer could contain sensitive information such as Elasticsearch documents or authentication details.	6.5	More Details
CVE-2021-2421	Vulnerability in the PeopleSoft Enterprise CS Campus Community product of Oracle PeopleSoft (component: Integration and Interfaces). Supported versions that are affected are 9.0 and 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise CS Campus Community. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise CS Campus Community 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-2021-2455	Vulnerability in the PeopleSoft Enterprise HCM Shared Components product of Oracle PeopleSoft (component: Person Search). The supported version that is affected is 9.2. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Shared Components. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise HCM Shared Components accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise HCM Shared Components accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N).	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22773	A CWE-620: Unverified Password Change vulnerability exists in EVlink City (EVC1S22P4 / EVC1S7P4 all versions prior to R8 V3.4.0.1), EVlink Parking (EVW2 / EVF2 / EV.2 all versions prior to R8 V3.4.0.1), and EVlink Smart Wallbox (EVB1A all versions prior to R8 V3.4.0.1) that could allow an attacker connected to the charging station web server to modify the password of a user.	6.5	More Details
CVE-2021-22770	A CWE-200: Information Exposure vulnerability exists in Easergy T300 with firmware V2.7.1 and older that exposes sensitive information to an actor not explicitly authorized to have access to that information.	6.5	More Details
CVE-2021-2404	Vulnerability in the PeopleSoft Enterprise HCM Candidate Gateway product of Oracle PeopleSoft (component: e-mail notification). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Candidate Gateway. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HCM Candidate Gateway accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HCM Candidate Gateway accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	6.5	More Details
CVE-2020-20219	Mikrotik RouterOs 6.44.6 (long-term tree) suffers from a memory corruption vulnerability in the /nova/bin/igmp-proxy process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).	6.5	More Details
CVE-2020-20221	Mikrotik RouterOs before 6.44.6 (long-term tree) suffers from an uncontrolled resource consumption vulnerability in the /nova/bin/cerm process. An authenticated remote attacker can cause a Denial of Service due to overloading the systems CPU.	6.5	More Details
CVE-2021-22728	A CWE-200: Information Exposure vulnerability exists in EVlink City (EVC1S22P4 / EVC1S7P4 all versions prior to R8 V3.4.0.1), EVlink Parking (EVW2 / EVF2 / EV.2 all versions prior to R8 V3.4.0.1), and EVlink Smart Wallbox (EVB1A all versions prior to R8 V3.4.0.1) that could cause disclosure of encrypted credentials when consulting the maintenance report.	6.5	More Details
CVE-2020-20262	Mikrotik RouterOs before 6.47 (stable tree) suffers from an assertion failure vulnerability in the /ram/pckg/security/nova/bin/ipsec process. An authenticated remote attacker can cause a Denial of Service due to an assertion failure via a crafted packet.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20106	Nessus Agent versions 8.2.5 and earlier were found to contain a privilege escalation vulnerability which could allow a Nessus administrator user to upload a specially crafted file that could lead to gaining administrator privileges on the Nessus host.	6.5	More Details
CVE-2021-2366	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versions that are affected are 17.12.0-17.12.20, 18.8.0-18.8.23, 19.12.0-19.12.14 and 20.12.0-20.12.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. While the vulnerability is in Primavera P6 Enterprise Project Portfolio Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera P6 Enterprise Project Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera P6 Enterprise Project Portfolio Management accessible data. CVSS 3.1 Base Score 6.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N).	6.4	More Details
CVE-2021-37159	hso_free_net_device in drivers/net/usb/hso.c in the Linux kernel through 5.13.4 calls unregister_netdev without checking for the NETREG_REGISTERED state, leading to a use-after-free and a double free.	6.4	More Details
CVE-2021-1518	A vulnerability in the REST API of Cisco Firepower Device Manager (FDM) On-Box Software could allow an authenticated, remote attacker to execute arbitrary code on the underlying operating system of an affected device. This vulnerability is due to insufficient sanitization of user input on specific REST API commands. An attacker could exploit this vulnerability by sending a crafted HTTP request to the API subsystem of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system. To exploit this vulnerability, an attacker would need valid low-privileged user credentials.	6.3	More Details
CVE-2021-35520	A Buffer Overflow in Thrift command handlers in IDEMIA Morpho Wave Compact and VisionPass devices before 2.6.2 allows physically proximate authenticated attackers to achieve code execution, denial of services, and information disclosure via serial ports.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1100	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager kernel mode driver (nvidia.ko), in which a pointer to a user-space buffer is not validated before it is dereferenced, which may lead to denial of service. This affects vGPU version 12.x (prior to 12.3), version 11.x (prior to 11.5) and version 8.x (prior 8.8).	6.2	More Details
CVE-2021-29149	A local bypass security restrictions vulnerability was discovered in Aruba CX 6200F Switch Series, Aruba 6300 Switch Series, Aruba 6400 Switch Series, Aruba 8320 Switch Series, Aruba 8325 Switch Series, Aruba 8400 Switch Series, Aruba CX 8360 Switch Series version(s): Aruba AOS-CX firmware: 10.04.xxxx - versions prior to 10.04.3070, 10.05.xxxx - versions prior to 10.05.0070, 10.06.xxxx - versions prior to 10.06.0110, 10.07.xxxx - versions prior to 10.07.0001. Aruba has released upgrades for Aruba AOS-CX devices that address this security vulnerability.	6.2	More Details
CVE-2021-1093	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in firmware where the driver contains an assert() or similar statement that can be triggered by an attacker, which leads to an application exit or other behavior that is more severe than necessary, and may lead to denial of service or system crash.	6.2	More Details
CVE-2021-30049	SysAid 20.3.64 b14 is affected by Cross Site Scripting (XSS) via a /KeepAlive.jsp?stamp= URI.	6.1	More Details
CVE-2021-37403	OX App Suite before 7.10.3-rev32 and 7.10.4 before 7.10.4-rev18 allows XSS via a code snippet (user-generated content) when a sharing link is created and an App Loader relative URL is used.	6.1	More Details
CVE-2021-29148	A local cross-site scripting (XSS) vulnerability was discovered in Aruba CX 6200F Switch Series, Aruba 6300 Switch Series, Aruba 6400 Switch Series, Aruba 8320 Switch Series, Aruba 8325 Switch Series, Aruba 8400 Switch Series, Aruba CX 8360 Switch Series version(s): Aruba AOS-CX firmware: 10.04.xxxx - versions prior to 10.04.3070, 10.05.xxxx - versions prior to 10.05.0070, 10.06.xxxx - versions prior to 10.06.0110, 10.07.xxxx - versions prior to 10.07.0001. Aruba has released upgrades for Aruba AOS-CX devices that address this security vulnerability.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2408	Vulnerability in the PeopleSoft Enterprise PT PeopleTools product of Oracle PeopleSoft (component: Notification Configuration). The supported version that is affected is 8.59. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PT PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PT PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PT 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-2021-2375	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime). Supported versions that are affected are 9.2.5.3 and prior. 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. 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-2021-26227	Cross-site scripting (XSS) vulnerability in SourceCodester CASAP Automated Enrollment System v 1.0 allows remote attackers to inject arbitrary web script or HTML via the student information parameters to edit_stud.php.	6.1	More Details
CVE-2021-26230	Cross-site scripting (XSS) vulnerability in SourceCodester CASAP Automated Enrollment System v 1.0 allows remote attackers to inject arbitrary web script or HTML via the user information to save_user.php.	6.1	More Details
CVE-2021-26698	OX App Suite before 7.10.3-rev32 and 7.10.4 before 7.10.4-rev18 allows XSS via a code snippet (user-generated content) when a sharing link is created and the dl parameter is used.	6.1	More Details
CVE-2021-37402	OX App Suite before 7.10.3-rev32 and 7.10.4 before 7.10.4-rev18 allows XSS via binary data that is mishandled when the legacy dataretrieval endpoint has been enabled.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1094	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape where an out of bounds array access may lead to denial of service or information disclosure.	6.1	More Details
CVE-2021-25197	Cross-site scripting (XSS) vulnerability in SourceCodester Content Management System v 1.0 allows remote attackers to inject arbitrary web script or HTML via the search parameter to content_management_system\admin\new_content.php	6.1	More Details
CVE-2021-2338	Vulnerability in the Siebel Apps - Marketing product of Oracle Siebel CRM (component: Email Marketing Stand-Alone). Supported versions that are affected are 21.5 and Prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel Apps - Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Siebel Apps - Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Siebel Apps - Marketing accessible data as well as unauthorized read access to a subset of Siebel Apps - Marketing 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-2021-2462	Vulnerability in the Oracle Commerce Service Center product of Oracle Commerce (component: Commerce Service Center). Supported versions that are affected are 11.0.0, 11.1.0, 11.2.0 and 11.3.0-11.3.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Service Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Service Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Service Center accessible data as well as unauthorized read access to a subset of Oracle Commerce Service Center 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-2020-22148	A stored cross site scripting (XSS) vulnerability in /admin.php?page=tags of Piwigo 2.10.1 allows attackers to execute arbitrary web scripts or HTML.	6.1	More Details
CVE-2020-22150	A cross site scripting (XSS) vulnerability in /admin.php?page=permalinks of Piwigo 2.10.1 allows attackers to execute arbitrary web scripts or HTML.	6.1	More Details
CVE-2021-22706	A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists in EVlink City (EVC1S22P4 / EVC1S7P4 all versions prior to R8 V3.4.0.1), EVlink Parking (EVW2 / EVF2 / EV.2 all versions prior to R8 V3.4.0.1), and EVlink Smart Wallbox (EVB1A all versions prior to R8 V3.4.0.1) that could allow an attacker to impersonate the user who manages the charging station or carry out actions on their behalf when crafted malicious parameters are submitted to the charging station web server.	6.1	More Details
CVE-2021-22723	A CWE-79: Improper Neutralization of Input During Web Page Generation (Cross-siteScripting) through Cross-Site Request Forgery (CSRF) vulnerability exists in EVlink City (EVC1S22P4 / EVC1S7P4 all versions prior to R8 V3.4.0.1), EVlink Parking (EVW2 / EVF2 / EV.2 all versions prior to R8 V3.4.0.1), and EVlink Smart Wallbox (EVB1A all versions prior to R8 V3.4.0.1) that could allow an attacker to impersonate the user who manages the charging station or carry out actions on their behalf when crafted malicious parameters are submitted to the charging station web server.	6.1	More Details
CVE-2021-26799	Cross Site Scripting (XSS) vulnerability in admin/files/edit in Omeka Classic <=2.7 allows remote attackers to inject arbitrary web script or HTML.	6.1	More Details
CVE-2021-27332	Cross-site scripting (XSS) vulnerability in SourceCodester CASAP Automated Enrollment System v 1.0 allows remote attackers to inject arbitrary web script or HTML via the class_name parameter to update_class.php.	6.1	More Details
CVE-2021-26224	Cross-site scripting (XSS) vulnerability in SourceCodester Fantastic-Blog-CMS V 1.0 allows remote attackers to inject arbitrary web script or HTML via the search field to search.php.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2417	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: GIS). Supported versions that are affected are 8.0.25 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 and unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:H).	6.0	More Details
CVE-2021-2442	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.24. 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. 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 6.0 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H).	6.0	More Details
CVE-2021-2389	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.34 and prior and 8.0.25 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 ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).	5.9	More Details
CVE-2021-32686	PJSIP is a free and open source multimedia communication library written in C language implementing standard based protocols such as SIP, SDP, RTP, STUN, TURN, and ICE. In PJSIP before version 2.11.1, there are a couple of issues found in the SSL socket. First, a race condition between callback and destroy, due to the accepted socket having no group lock. Second, the SSL socket parent/listener may get destroyed during handshake. Both issues were reported to happen intermittently in heavy load TLS connections. They cause a crash, resulting in a denial of service. These are fixed in version 2.11.1.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2368	Vulnerability in the Siebel CRM product of Oracle Siebel CRM (component: Siebel Core - Server Infrastructure). Supported versions that are affected are 21.5 and Prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Siebel CRM. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel CRM 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-2021-2390	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.34 and prior and 8.0.25 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 ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).	5.9	More Details
CVE-2021-35521	A path traversal in Thrift command handlers in IDEMIA Morpho Wave Compact and VisionPass devices before 2.6.2 allows remote authenticated attackers to achieve denial of services and information disclosure via TCP/IP packets.	5.9	More Details
CVE-2021-2356	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.34 and prior and 8.0.25 and prior. Difficult to exploit 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 as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:H).	5.9	More Details
CVE-2021-32791	mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2323	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Flex-Branch). Supported versions that are affected are 12.3, 12.4, 14.0-14.4 and . Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking 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-2021-2429	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.25 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 ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).	5.9	More Details
CVE-2021-21406	Combodo iTop is an open source, web based IT Service Management tool. In versions prior to 2.7.4, there is a command injection vulnerability in the Setup Wizard when providing Graphviz executable path. The vulnerability is patched in version 2.7.4 and 3.0.0.	5.8	More Details
CVE-2021-22784	A CWE-306: Missing Authentication for Critical Function vulnerability exists in C-Bus Toolkit v1.15.8 and prior that could allow an attacker to use a crafted webpage to obtain remote access to the system.	5.7	More Details
CVE-2021-2445	Vulnerability in the Hyperion Infrastructure Technology product of Oracle Hyperion (component: Lifecycle Management). The supported version that is affected is 11.2.5.0. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Hyperion Infrastructure Technology. 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 Hyperion Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 5.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:N).	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34700	A vulnerability in the CLI interface of Cisco SD-WAN vManage Software could allow an authenticated, local attacker to read arbitrary files on the underlying file system of an affected system. This vulnerability exists because access to sensitive information on an affected system is not sufficiently controlled. An attacker could exploit this vulnerability by gaining unauthorized access to sensitive information on an affected system. A successful exploit could allow the attacker to create forged authentication requests and gain unauthorized access to the web UI of an affected system.	5.5	More Details
CVE-2020-19466	An issue has been found in function DCTStream::transformDataUnit in PDF2JSON 0.70 that allows attackers to cause a Denial of Service due to an invalid read of size 1 .	5.5	More Details
CVE-2020-19471	An issue has been found in function DCTStream::decodeImage in PDF2JSON 0.70 that allows attackers to cause a Denial of Service due to an invalid read of size 4 .	5.5	More Details
CVE-2020-19490	tinyexr 0.9.5 has a integer overflow over-write in tinyexr::DecodePixelData in tinyexr.h, related to OpenEXR code.	5.5	More Details
CVE-2020-19488	An issue was discovered in box_code_apple.c:119 in Gpac MP4Box 0.8.0, allows attackers to cause a Denial of Service due to an invalid read on function ilst_item_Read.	5.5	More Details
CVE-2020-19467	An issue has been found in function DCTStream::transformDataUnit in PDF2JSON 0.70 that allows attackers to cause a Denial of Service due to an Illegal Use After Free .	5.5	More Details
CVE-2020-19470	An issue has been found in function DCTStream::getChar in PDF2JSON 0.70 that allows attackers to cause a Denial of Service due to a NULL pointer dereference (invalid read of size 1) .	5.5	More Details
CVE-2020-19472	An issue has been found in function DCTStream::readHuffSym in PDF2JSON 0.70 that allows attackers to cause a Denial of Service due to an invalid read of size 2 .	5.5	More Details
CVE-2021-25701	The fUSBHub driver in the PCoIP Software Client prior to version 21.07.0 had an error in object management during the handling of a variety of IOCTLs, which allowed an attacker to cause a denial of service.	5.5	More Details
CVE-2020-19481	An issue was discovered in GPAC before 0.8.0, as demonstrated by MP4Box. It contains an invalid memory read in gf_m2ts_process_pmt in media_tools/mpegts.c that can cause a denial of service via a crafted MP4 file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-19475	An issue has been found in function CCITTFaxStream::lookChar in PDF2JSON 0.70 that allows attackers to cause a Denial of Service due to an invalid write of size 2 .	5.5	More Details
CVE-2020-19473	An issue has been found in function DCTStream::decodeImage in PDF2JSON 0.70 that allows attackers to cause a Denial of Service due to an uncaught floating point exception.	5.5	More Details
CVE-2020-19474	An issue has been found in function Gfx::doShowText in PDF2JSON 0.70 that allows attackers to cause a Denial of Service due to an Use After Free .	5.5	More Details
CVE-2021-1101	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it can dereference a NULL pointer, which may lead to denial of service. This affects vGPU version 12.x (prior to 12.3), version 11.x (prior to 11.5) and version 8.x (prior 8.8).	5.5	More Details
CVE-2020-19468	An issue has been found in function EmbedStream::getChar in PDF2JSON 0.70 that allows attackers to cause a Denial of Service due to a null pointer derefenrece (invalid read of size 8) .	5.5	More Details
CVE-2020-19465	An issue has been found in function ObjectStream::getObject in PDF2JSON 0.70 that allows attackers to cause a Denial of Service due to an invalid read of size 4 .	5.5	More Details
CVE-2020-19464	An issue has been found in function XRef::fetch in PDF2JSON 0.70 that allows attackers to cause a Denial of Service due to a stack overflow .	5.5	More Details
CVE-2020-7389	Sage X3 System CHAINE Variable Script Command Injection. An authenticated user with developer access can pass OS commands via this variable used by the web application. Note, this developer configuration should not be deployed in production.	5.5	More Details
CVE-2020-19609	Artifex MuPDF before 1.18.0 has a heap based buffer over-write in tiff_expand_colormap() function when parsing TIFF files allowing attackers to cause a denial of service.	5.5	More Details
CVE-2021-37220	MuPDF through 1.18.1 has an out-of-bounds write because the cached color converter does not properly consider the maximum key size of a hash table. This can, for example, be seen with crafted "mutool draw" input.	5.5	More Details
CVE-2020-19469	An issue has been found in function DCTStream::reset in PDF2JSON 0.70 that allows attackers to cause a Denial of Service due to an invalid write of size 8 .	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37452	NCH Quorum v2.03 and earlier allows local users to discover cleartext login information relating to users by reading the local .dat configuration files.	5.5	More Details
CVE-2021-1102	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it can lead to floating point exceptions, which may lead to denial of service. This affects vGPU version 12.x (prior to 12.3), version 11.x (prior to 11.5) and version 8.x (prior 8.8).	5.5	More Details
CVE-2020-19463	An issue has been found in function vfprintf in PDF2JSON 0.70 that allows attackers to cause a Denial of Service due to a stack overflow.	5.5	More Details
CVE-2021-1095	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handlers for all control calls with embedded parameters where dereferencing an untrusted pointer may lead to denial of service.	5.5	More Details
CVE-2021-1096	NVIDIA Windows GPU Display Driver for Windows contains a vulnerability in the NVIDIA kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape where dereferencing a NULL pointer may lead to a system crash.	5.5	More Details
CVE-2021-3159	A stored cross site scripting (XSS) vulnerability in the /sys/attachment/uploaderServlet component of Landray EKP V12.0.9.R.20160325 allows attackers to execute arbitrary web scripts or HTML via a crafted SVG, SHTML, or MHT file.	5.4	More Details
CVE-2021-37453	Cross Site Scripting (XSS) exists in NCH Axon PBX v2.22 and earlier via the extension name (stored).	5.4	More Details
CVE-2021-37454	Cross Site Scripting (XSS) exists in NCH Axon PBX v2.22 and earlier via the line name (stored).	5.4	More Details
CVE-2021-37467	In NCH Quorum v2.03 and earlier, XSS exists via /conferencebrowseuploadfile?confid= (reflected).	5.4	More Details
CVE-2021-25791	Multiple stored cross site scripting (XSS) vulnerabilities in the "Update Profile" module of Online Doctor Appointment System 1.0 allows authenticated attackers to execute arbitrary web scripts or HTML via crafted payloads in the First Name, Last Name, and Address text fields.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37466	In NCH Quorum v2.03 and earlier, XSS exists via /conference?id= (reflected).	5.4	More Details
CVE-2021-25790	Multiple stored cross site scripting (XSS) vulnerabilities in the "Register" module of House Rental and Property Listing 1.0 allows authenticated attackers to execute arbitrary web scripts or HTML via crafted payloads in all text fields except for Phone Number and Alternate Phone Number.	5.4	More Details
CVE-2021-37455	Cross Site Scripting (XSS) exists in NCH Axon PBX v2.22 and earlier via the outbound dialing plan (stored).	5.4	More Details
CVE-2021-37456	Cross Site Scripting (XSS) exists in NCH Axon PBX v2.22 and earlier via the blacklist IP address (stored).	5.4	More Details
CVE-2021-25204	Cross-site scripting (XSS) vulnerability in SourceCodester E-Commerce Website v 1.0 allows remote attackers to inject arbitrary web script or HTM via the subject field to feedback_process.php.	5.4	More Details
CVE-2021-37457	Cross Site Scripting (XSS) exists in NCH Axon PBX v2.22 and earlier via the SipRule field (stored).	5.4	More Details
CVE-2021-37464	In NCH Quorum v2.03 and earlier, XSS exists via Conference Description (stored).	5.4	More Details
CVE-2021-2345	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Tools and Frameworks). The supported version that is affected is 11.3.1.5. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized read access to a subset of Oracle Commerce Guided Search / Oracle Commerce Experience Manager 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-2021-37463	In NCH Quorum v2.03 and earlier, XSS exists via User Display Name (stored).	5.4	More Details
CVE-2021-37462	Cross Site Scripting (XSS) exists in NCH Axon PBX v2.22 and earlier via /ipblacklist?errorip= (reflected).	5.4	More Details
CVE-2021-37461	Cross Site Scripting (XSS) exists in NCH Axon PBX v2.22 and earlier via /extensionsinstruction?id= (reflected).	5.4	More Details
CVE-2021-37460	Cross Site Scripting (XSS) exists in NCH Axon PBX v2.22 and earlier via /planprop?id= (reflected).	5.4	More Details
CVE-2020-23238	Cross Site Scripting (XSS) vulnerability in Evolution CMS 2.0.2 via the Document Manager feature.	5.4	More Details
CVE-2021-37459	Cross Site Scripting (XSS) exists in NCH Axon PBX v2.22 and earlier via the customer name field (stored).	5.4	More Details
CVE-2021-2346	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Tools and Frameworks). The supported version that is affected is 11.3.1.5. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized read access to a subset of Oracle Commerce Guided Search / Oracle Commerce Experience Manager 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-2021-37458	Cross Site Scripting (XSS) exists in NCH Axon PBX v2.22 and earlier via the primary phone field (stored).	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37465	In NCH Quorum v2.03 and earlier, XSS exists via /uploaddoc?id= (reflected).	5.4	More Details
CVE-2021-37392	In RPCMS v1.8 and below, the "nickname" variable is not properly sanitized before being displayed on page. When the API functions are enabled, the attacker can use API to update user nickname with XSS payload and achieve stored XSS. Users who view the articles published by the injected user will trigger the XSS.	5.4	More Details
CVE-2021-2460	Vulnerability in the Oracle Application Express Data Reporter component of Oracle Database Server. The supported version that is affected is Prior to 21.1.0.00.04. Easily exploitable vulnerability allows low privileged attacker having Valid User Account privilege with network access via HTTP to compromise Oracle Application Express Data Reporter. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express Data Reporter, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Express Data Reporter accessible data as well as unauthorized read access to a subset of Oracle Application Express Data Reporter 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-2021-26699	OX App Suite before 7.10.3-rev4 and 7.10.4 before 7.10.4-rev4 allows SSRF via a shared SVG document that is mishandled by the imageconverter component when the .png extension is used.	5.4	More Details
CVE-2021-37534	app/View/GalaxyClusters/add.ctp in MISP 2.4.146 allows Stored XSS when forking a galaxy cluster.	5.4	More Details
CVE-2021-23408	This affects the package com.graphhopper:graphhopper-web-bundle before 3.2, from 4.0-pre1 and before 4.0. The URL parser could be tricked into adding or modifying properties of Object.prototype using a constructor or __proto__ payload.	5.4	More Details
CVE-2021-20560	IBM Sterling Connect:Direct Browser User Interface 1.4.1.1 and 1.5.0.2 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 199229.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1599	A vulnerability in the web-based management interface of Cisco Unified Customer Voice Portal (CVP) could allow an authenticated, remote attacker to perform a cross-site scripting (XSS) attack against a user. This vulnerability is due to insufficient input validation of a parameter that is used by the web-based management interface. An attacker could exploit this vulnerability by persuading a user to click a malicious link. A successful exploit could allow the attacker to execute arbitrary code in the context of the interface, access sensitive, browser-based information, or cause an affected device to reboot under certain conditions.	5.4	More Details
CVE-2021-22722	A CWE-79: Improper Neutralization of Input During Web Page Generation ('Stored Cross-site Scripting') vulnerability exists in EVlink City (EVC1S22P4 / EVC1S7P4 all versions prior to R8 V3.4.0.1), EVlink Parking (EVW2 / EVF2 / EV.2 all versions prior to R8 V3.4.0.1), and EVlink Smart Wallbox (EVB1A all versions prior to R8 V3.4.0.1) that could cause code injection when importing a CSV file or changing station parameters.	5.4	More Details
CVE-2021-36563	The CheckMK management web console (versions 1.5.0 to 2.0.0) does not sanitise user input in various parameters of the WATO module. This allows an attacker to open a backdoor on the device with HTML content and interpreted by the browser (such as JavaScript or other client-side scripts), the XSS payload will be triggered when the user accesses some specific sections of the application. In the same sense a very dangerous potential way would be when an attacker who has the monitor role (not administrator) manages to get a stored XSS to steal the secretAutomation (for the use of the API in administrator mode) and thus be able to create another administrator user who has high privileges on the CheckMK monitoring web console. Another way is that persistent XSS allows an attacker to modify the displayed content or change the victim's information. Successful exploitation requires access to the web management interface, either with valid credentials or with a hijacked session.	5.4	More Details
CVE-2021-37449	Cross Site Scripting (XSS) exists in NCH IVM Attendant v5.12 and earlier via /ogmlist?folder= (reflected).	5.4	More Details
CVE-2021-37450	Cross Site Scripting (XSS) exists in NCH IVM Attendant v5.12 and earlier via /ogmprop?id= (reflected).	5.4	More Details
CVE-2021-37448	Cross Site Scripting (XSS) exists in NCH IVM Attendant v5.12 and earlier via the Mailbox name (stored).	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23411	Affected versions of this package are vulnerable to Cross-site Scripting (XSS) via the main functionality. It accepts input that can result in the output (an anchor a tag) containing undesirable Javascript code that can be executed upon user interaction.	5.4	More Details
CVE-2021-20562	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 5.2.6.5_3 and 6.1.0.0 through 6.1.0.2 vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199232.	5.4	More Details
CVE-2021-37470	In NCH WebDictate v2.13, persistent Cross Site Scripting (XSS) exists in the Recipient Name field. An authenticated user can add or modify the affected field to inject arbitrary JavaScript.	5.4	More Details
CVE-2021-37451	Cross Site Scripting (XSS) exists in NCH IVM Attendant v5.12 and earlier via /msglist?mbx= (reflected).	5.4	More Details
CVE-2021-37393	In RPCMS v1.8 and below, the "nickname" variable is not properly sanitized before being displayed on page. Attacker can use "update password" function to inject XSS payloads into nickname variable, and achieve stored XSS. Users who view the articles published by the injected user will trigger the XSS.	5.4	More Details
CVE-2021-2373	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime). Supported versions that are affected are 9.2.5.3 and Prior. Easily exploitable vulnerability allows low privileged 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. 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 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-2021-2401	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: E-Business Suite - XDO). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 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 BI Publisher. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle BI Publisher accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2021-2457	Vulnerability in the Identity Manager product of Oracle Fusion Middleware (component: Request Management & Workflow). The supported version that is affected is 11.1.2.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Identity Manager. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Identity Manager accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2021-23413	This affects the package jszip before 3.7.0. Crafting a new zip file with filenames set to Object prototype values (e.g __proto__, toString, etc) results in a returned object with a modified prototype instance.	5.3	More Details
CVE-2020-21932	A vulnerability in /Login.html of Motorola CX2 router CX 1.0.2 Build 20190508 Rel.97360n allows attackers to bypass login and obtain a partially authorized token and uid.	5.3	More Details
CVE-2021-2407	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.57, 8.58 and 8.59. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2020-21936	An issue in HNAP1/GetMultipleHNAPs of Motorola CX2 router CX 1.0.2 Build 20190508 Rel.97360n allows attackers to access the components GetStationSettings, GetWebsiteFilterSettings and GetNetworkSettings without authentication.	5.3	More Details
CVE-2021-25809	UCMS 1.5.0 was discovered to contain a physical path leakage via an error message returned by the adminchannelscache() function in top.php.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2403	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2021-3664	url-parse is vulnerable to URL Redirection to Untrusted Site	5.3	More Details
CVE-2021-29766	IBM i2 Analyst's Notebook Premium (IBM i2 Analyze 4.3.0, 4.3.1, and 4.3.2) 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: 202680.	5.3	More Details
CVE-2021-29767	IBM i2 Analyst's Notebook Premium 9.2.0, 9.2.1, and 9.2.2 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: 202681.	5.3	More Details
CVE-2021-20333	Sending specially crafted commands to a MongoDB Server may result in artificial log entries being generated or for log entries to be split. This issue affects MongoDB Server v3.6 versions prior to 3.6.20; MongoDB Server v4.0 versions prior to 4.0.21 and MongoDB Server v4.2 versions prior to 4.2.10.	5.3	More Details
CVE-2021-20430	IBM i2 Analyst's Notebook Premium (IBM i2 Analyze 4.3.0, 4.3.1, and 4.3.2) 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: 196341.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7387	Sage X3 Installation Pathname Disclosure. A specially crafted packet can elicit a response from the AdxDSrv.exe component that reveals the installation directory of the product. Note that this vulnerability can be combined with CVE-2020-7388 to achieve full RCE. This issue was fixed in AdxAdmin 93.2.53, which ships with updates for on-premises versions of Sage X3 Version 9 (components shipped with Syracuse 9.22.7.2 and later), Sage X3 HR & Payroll Version 9 (those components that ship with Syracuse 9.24.1.3), Version 11 (components shipped with Syracuse 11.25.2.6 and later), and Version 12 (components shipped with Syracuse 12.10.2.8 and later) of Sage X3. Other on-premises versions of Sage X3 are unsupported by the vendor.	5.3	More Details
CVE-2021-1614	A vulnerability in the Multiprotocol Label Switching (MPLS) packet handling function of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to gain access to information stored in MPLS buffer memory. This vulnerability is due to insufficient handling of malformed MPLS packets that are processed by a device that is running Cisco SD-WAN Software. An attacker could exploit this vulnerability by sending a crafted MPLS packet to an affected device that is running Cisco SD-WAN Software or Cisco SD-WAN vManage Software. A successful exploit could allow the attacker to gain unauthorized access to sensitive information.	5.3	More Details
CVE-2021-22721	A CWE-200: Information Exposure vulnerability exists in EVlink City (EVC1S22P4 / EVC1S7P4 all versions prior to R8 V3.4.0.1), EVlink Parking (EVW2 / EVF2 / EV.2 all versions prior to R8 V3.4.0.1), and EVlink Smart Wallbox (EVB1A all versions prior to R8 V3.4.0.1) that could allow an attacker to get limited knowledge of javascript code when crafted malicious parameters are submitted to the charging station web server.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32785	mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (`OIDCCacheEncrypt off`, `OIDCSessionType server-cache`, `OIDCCacheType redis`), `mod_auth_openidc` wrongly performed argument interpolation before passing Redis requests to `hiredis`, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the `hiredis` API. As a workaround, this vulnerability can be mitigated by setting `OIDCCacheEncrypt` to `on`, as cache keys are cryptographically hashed before use when this option is enabled.	5.3	More Details
CVE-2021-2347	Vulnerability in the Hyperion Infrastructure Technology product of Oracle Hyperion (component: Lifecycle Management). The supported version that is affected is 11.2.5.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Hyperion Infrastructure Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Hyperion Infrastructure Technology accessible data as well as unauthorized update, insert or delete access to some of Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 5.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:L/A:N).	5.2	More Details
CVE-2021-21440	Generated Support Bundles contains private S/MIME and PGP keys if containing folder is not hidden. This issue affects: OTRS AG ((OTRS)) Community Edition 6.0.x version 6.0.1 and later versions. OTRS AG OTRS 7.0.x version 7.0.27 and prior versions; 8.0.x version 8.0.14 and prior versions.	5.2	More Details
CVE-2021-2385	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.34 and prior and 8.0.25 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 Number	Description	Base Score	Reference
CVE-2021-2339	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.25 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-2021-32790	Woocommerce is an open source eCommerce plugin for WordPress. An SQL injection vulnerability impacts all WooCommerce sites running the WooCommerce plugin between version 3.3.0 and 3.3.6. Malicious actors (already) having admin access, or API keys to the WooCommerce site can exploit vulnerable endpoints of `/wp-json/wc/v3/webhooks`, `/wp-json/wc/v2/webhooks` and other webhook listing API. Read-only SQL queries can be executed using this exploit, while data will not be returned, by carefully crafting `search` parameter information can be disclosed using timing and related attacks. Version 3.3.6 is the earliest version of Woocommerce with a patch for this vulnerability. There are no known workarounds other than upgrading.	4.9	More Details
CVE-2021-2440	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.25 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-2021-2441	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 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-2021-2402	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Locking). Supported versions that are affected are 8.0.25 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-2021-2333	Vulnerability in the Oracle XML DB component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Easily exploitable vulnerability allows high privileged attacker having Alter User privilege with network access via Oracle Net to compromise Oracle XML DB. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle XML DB accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	4.9	More Details
CVE-2021-2427	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 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-2021-2384	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 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-2021-2426	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 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-2021-2383	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 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-2021-2412	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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-2021-2425	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 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-2021-2437	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 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-2021-2399	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.25 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-2021-2418	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 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-2021-2370	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.25 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-2021-2424	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.25 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-2021-2367	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 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-2021-2410	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 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-2021-2387	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 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-2021-2354	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Federated). Supported versions that are affected are 8.0.25 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-2021-2342	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.34 and prior and 8.0.25 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-2021-2422	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.25 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-2021-2444	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 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-2021-2352	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.25 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-2021-2358	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Rest interfaces for Access Mgr). The supported version that is affected is 11.1.2.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTPS to compromise Oracle Access Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Access Manager accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	4.9	More Details
CVE-2021-2357	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 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-2020-23240	Cross Site Scripting (XSS) vulnerablity in CMS Made Simple 2.2.14 via the Logic field in the Content Manager feature.	4.8	More Details
CVE-2020-23234	Cross Site Scripting (XSS) vulnerabiity exists in LavaLite CMS 5.8.0 via the Menu Blocks feature, which can be bypassed by using HTML event handlers, such as "ontoggle,".	4.8	More Details
CVE-2020-23239	Cross Site Scripting (XSS) vulnerability in Textpattern CMS 4.8.1 via Custom fields in the Menu Preferences feature.	4.8	More Details
CVE-2020-23243	Cross Site Scripting (XSS) vulnerability in NavigateCMS NavigateCMS 2.9 via the name="wrong_path_redirect" feature.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-23242	Cross Site Scripting (XSS) vulnerability in NavigateCMS 2.9 when performing a Create or Edit via the Tools feature.	4.8	More Details
CVE-2020-23241	Cross Site Scripting (XSS) vulnerability in CMS Made Simple 2.2.14 in "Extra" via 'News > Article" feature.	4.8	More Details
CVE-2021-32786	mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, `oidc_validate_redirect_url()` does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring `mod_auth_openidc` to only allow redirection whose destination matches a given regular expression.	4.7	More Details
CVE-2021-2324	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Loans And Deposits). Supported versions that are affected are 12.0-12.4, 14.0-14.4 and . Easily exploitable 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 update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N).	4.6	More Details
CVE-2021-34261	An issue in USBH_ParseCfgDesc() of STMicroelectronics STM32Cube Middleware v1.8.0 and below causes a denial of service due to the system hanging when trying to set a remote wake-up feature.	4.6	More Details
CVE-2021-34267	An in the USBH_MSC_InterfaceInit() function of STMicroelectronics STM32Cube Middleware v1.8.0 and below causes a denial of service (DOS) when the system tries to communicate with the connected endpoint.	4.6	More Details
CVE-2021-34268	An issue in the USBH_ParseDevDesc() function of STMicroelectronics STM32Cube Middleware v1.8.0 and below causes a denial of service (DOS) via a malformed USB device packet.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7390	Sage X3 Stored XSS Vulnerability on ‘Edit’ Page of User Profile. An authenticated user can pass XSS strings the "First Name," "Last Name," and "Email Address" fields of this web application component. Updates are available for on-premises versions of Version 12 (components shipped with Syracuse 12.10.0 and later) of Sage X3. Other on-premises versions of Sage X3 are unaffected or unsupported by the vendor.	4.6	More Details
CVE-2021-21442	In the project create screen it's possible to inject malicious JS code to the certain fields. The code might be executed in the Reporting screen. This issue affects: OTRS AG Time Accounting: 7.0.x versions prior to 7.0.19.	4.5	More Details
CVE-2021-1103	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it can dereference a NULL pointer, which may lead to denial of service. This affects vGPU version 12.x (prior to 12.3), version 11.x (prior to 11.5) and version 8.x (prior 8.8).	4.4	More Details
CVE-2021-2353	Vulnerability in the Siebel Core - Server Framework product of Oracle Siebel CRM (component: Loging). Supported versions that are affected are 21.5 and Prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Siebel Core - Server Framework executes to compromise Siebel Core - Server Framework. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel Core - Server Framework accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	4.4	More Details
CVE-2021-2372	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.34 and prior and 8.0.25 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-2021-29784	IBM i2 Analyze 4.3.0, 4.3.1, and 4.3.2 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: 203168.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29769	IBM i2 Analyst's Notebook Premium (IBM i2 Analyze 4.3.0, 4.3.1, and 4.3.2) does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 202769.	4.3	More Details
CVE-2021-2348	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Tools and Frameworks). The supported version that is affected is 11.3.1.5. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	4.3	More Details
CVE-2021-2386	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versions that are affected are 20.12.0-20.12.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Primavera P6 Enterprise Project Portfolio Management accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	4.3	More Details
CVE-2021-32788	Discourse is an open source discussion platform. In versions prior to 2.7.7 there are two bugs which led to the post creator of a whisper post being revealed to non-staff users. 1: Staff users that creates a whisper post in a personal message is revealed to non-staff participants of the personal message even though the whisper post cannot be seen by them. 2: When a whisper post is before the last post in a post stream, deleting the last post will result in the creator of the whisper post to be revealed to non-staff users as the last poster of the topic.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2377	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: SQR). Supported versions that are affected are 8.57, 8.58 and 8.59. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	4.3	More Details
CVE-2021-32748	Nextcloud Richdocuments in an open source self hosted online office. Nextcloud uses the WOPI ("Web Application Open Platform Interface") protocol to communicate with the Collabora Editor, the communication between these two services was not protected by a credentials or IP check. Whilst this does not result in gaining access to data that the user has not yet access to, it can result in a bypass of any enforced watermark on documents as described on the [Nextcloud Virtual Data Room] (https://nextcloud.com/virtual-data-room/) website and [our documentation](https://portal.nextcloud.com/article/nextcloud-and-virtual-data-room-configuration-59.html). The Nextcloud Richdocuments releases 3.8.3 and 4.2.0 add an additional admin settings for an allowlist of IP addresses that can access the WOPI API. We recommend upgrading and configuring the allowlist to a list of Collabora servers. There is no known workaround. Note that this primarily results a bypass of any configured watermark or download protection using File Access Control. If you do not require or rely on these as a security feature no immediate action is required on your end.	4.3	More Details
CVE-2021-2438	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Easily exploitable vulnerability allows low privileged attacker having Create Procedure privilege with network access via Oracle Net to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java VM. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2439	Vulnerability in the Oracle Hyperion BI+ product of Oracle Hyperion (component: UI and Visualization). Supported versions that are affected are 11.1.2.4 and 11.2.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion BI+. 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 Oracle Hyperion BI+ accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N).	4.3	More Details
CVE-2021-2369	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Library). Supported versions that are affected are Java SE: 7u301, 8u291, 11.0.11, 16.0.1; Oracle GraalVM Enterprise Edition: 20.3.2 and 21.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).	4.3	More Details
CVE-2021-2330	Vulnerability in the Core RDBMS component of Oracle Database Server. The supported version that is affected is 19c. Easily exploitable vulnerability allows low privileged attacker having Create Table privilege with network access via Oracle Net to compromise Core RDBMS. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Core RDBMS. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	4.3	More Details
CVE-2021-2343	Vulnerability in the Oracle Workflow product of Oracle E-Business Suite (component: Workflow Notification Mailer). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Workflow. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Workflow accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37446	In NCH Quorum v2.03 and earlier, an authenticated user can use directory traversal via documentprop?file=/.. for file reading.	4.3	More Details
CVE-2021-37436	Amazon Echo Dot devices through 2021-07-02 sometimes allow attackers, who have physical access to a device after a factory reset, to obtain sensitive information via a series of complex hardware and software attacks. NOTE: reportedly, there were vendor marketing statements about safely removing personal content via a factory reset. Also, the vendor has reportedly indicated that they are working on mitigations.	4.2	More Details
CVE-2021-2374	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.25 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes 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 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N).	4.1	More Details
CVE-2021-2381	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. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.1 Base Score 3.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L).	3.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2448	Vulnerability in the Oracle Financial Services Crime and Compliance Investigation Hub product of Oracle Financial Services Applications (component: Reports). The supported version that is affected is 20.1.2. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Financial Services Crime and Compliance Investigation Hub executes to compromise Oracle Financial Services Crime and Compliance Investigation Hub. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Crime and Compliance Investigation Hub, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Crime and Compliance Investigation Hub accessible data as well as unauthorized read access to a subset of Oracle Financial Services Crime and Compliance Investigation Hub accessible data. CVSS 3.1 Base Score 3.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:C/C:L/I:L/A:N).	3.7	More Details
CVE-2021-2411	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: JS module). Supported versions that are affected are 8.0.25 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Cluster. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. 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-2021-2432	Vulnerability in the Java SE product of Oracle Java SE (component: JNDI). The supported version that is affected is Java SE: 7u301. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. 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 Number	Description	Base Score	Reference
CVE-2021-2336	Vulnerability in the Oracle Database - Enterprise Edition Data Redaction component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Oracle Database - Enterprise Edition Data Redaction. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Database - Enterprise Edition Data Redaction accessible data. CVSS 3.1 Base Score 3.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N).	3.5	More Details
CVE-2021-2335	Vulnerability in the Oracle Database - Enterprise Edition Data Redaction component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Oracle Database - Enterprise Edition Data Redaction. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Database - Enterprise Edition Data Redaction accessible data. CVSS 3.1 Base Score 3.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N).	3.5	More Details
CVE-2021-3619	Rapid7 Velociraptor 0.5.9 and prior is vulnerable to a post-authentication persistent cross-site scripting (XSS) issue, where an authenticated user could abuse MIME filetype sniffing to embed executable code on a malicious upload. This issue was fixed in version 0.6.0. Note that login rights to Velociraptor is nearly always reserved for trusted and verified users with IT security backgrounds.	3.5	More Details
CVE-2021-36091	Agents are able to list appointments in the calendars without required permissions. This issue affects: OTRS AG ((OTRS)) Community Edition: 6.0.x version 6.0.1 and later versions. OTRS AG OTRS: 7.0.x versions prior to 7.0.27.	3.5	More Details
CVE-2021-35030	A vulnerability was found in the CGI program in Zyxel GS1900-8 firmware version V2.60, that did not properly sterilize packet contents and could allow an authenticated, local user to perform a cross-site scripting (XSS) attack via a crafted LLDP packet.	3.5	More Details
CVE-2021-21443	Agents are able to list customer user emails without required permissions in the bulk action screen. This issue affects: OTRS AG ((OTRS)) Community Edition: 6.0.x version 6.0.1 and later versions. OTRS AG OTRS: 7.0.x versions prior to 7.0.27.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2334	Vulnerability in the Oracle Database - Enterprise Edition Data Redaction component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Oracle Database - Enterprise Edition Data Redaction. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Database - Enterprise Edition Data Redaction accessible data. CVSS 3.1 Base Score 3.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N).	3.5	More Details
CVE-2021-37468	NCH Reflect CRM 3.01 allows local users to discover cleartext user account information by reading the configuration files.	3.3	More Details
CVE-2021-2341	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u301, 8u291, 11.0.11, 16.0.1; Oracle GraalVM Enterprise Edition: 20.3.2 and 21.1.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. 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 Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).	3.1	More Details
CVE-2021-32792	mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using `OIDCPreservePost On`.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2340	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Memcached). Supported versions that are affected are 8.0.25 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-2021-2326	Vulnerability in the Database Vault component of Oracle Database Server. Supported versions that are affected are 12.2.0.1 and 19c. Easily exploitable vulnerability allows high privileged attacker having DBA privilege with network access via Oracle Net to compromise Database Vault. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Database Vault accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).	2.7	More Details
CVE-2018-11665	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2018-11659	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2018-11661	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2018-11662	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2021-23897	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability. However, the number was once accidentally misused to refer to the vulnerability that has the proper number of CVE-2021-31830. Notes: none	N/A	More Details
CVE-2018-11663	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-11664	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2021-34368	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2018-11666	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2018-11668	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2018-11669	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2019-9983	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2021-34365	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2021-34366	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2021-34367	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2021-23410	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-2021-31291	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-29457. Reason: This candidate is a duplicate of CVE-2021-29457. Notes: All CVE users should reference CVE-2021-29457 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37438	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