SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 27 January 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-2020-6779	Use of Hard-coded Credentials in the database of Bosch FSM-2500 server and Bosch FSM-5000 server up to and including version 5.2 allows an unauthenticated remote attacker to log into the database with admin-privileges. This may result in complete compromise of the confidentiality and integrity of the stored data as well as a high availability impact on the database itself. In addition, an attacker may execute arbitrary commands on the underlying operating system.	10.0	More Details
CVE-2021-3110	The store system in PrestaShop 1.7.7.0 allows time-based boolean SQL injection via the module=productcomments controller=CommentGrade id_products[] parameter.	9.8	More Details
CVE-2020-35263	EgavilanMedia User Registration & Login System 1.0 is affected by SQL injection to the admin panel, which may allow arbitrary code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14756	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Core Components). 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 IIOP, T3 to compromise Oracle Coherence. Successful attacks of this vulnerability can result in takeover of Oracle Coherence. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2020-3686	Possible memory out of bound issue during music playback when an incorrect bit stream content is copied into array without checking the length of array in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	9.8	More Details
CVE-2020-3691	Possible out of bound memory access in audio due to integer underflow while processing modified contents in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	9.8	More Details
CVE-2020-4958	IBM Security Identity Governance and Intelligence 5.2.6 does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources. IBM X-Force ID: 192209.	9.8	More Details
CVE-2020-20269	A specially crafted Markdown document could cause the execution of malicious JavaScript code in Caret Editor before 4.0.0-rc22.	9.8	More Details
CVE-2020-23262	An issue was discovered in ming-soft MCMS v5.0, where a malicious user can exploit SQL injection without logging in through /mcms/view.do.	9.8	More Details
CVE-2020-23448	newbee-mall all versions are affected by incorrect access control to remotely gain privileges through AdminLoginInterceptor.java. The authentication logic of the system's background /admin is in code AdminLoginInterceptor, which can be bypassed.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27539	Heap overflow with full parsing of HTTP respose in Rostelecom CS-C2SHW 5.0.082.1. AgentUpdater service has a self-written HTTP parser and builder. HTTP parser has a heap buffer overflow (OOB write). In default configuration camera parses responses only from HTTPS URLs from config file, so vulnerable code is unreachable and one more bug required to reach it.	9.8	More Details
CVE-2020-27540	Bash injection vulnerability and bypass of signature verification in Rostelecom CS-C2SHW 5.0.082.1. The camera reads firmware update configuration from SD card file vc\version.json. fw-sign parameter and from this configuration is directly inserted into a bash command. Firmware update is run automatically if there is special file on the inserted SD card.	9.8	More Details
CVE-2020-27583	IBM InfoSphere Information Server 8.5.0.0 is affected by deserialization of untrusted data which could allow remote unauthenticated attackers to execute arbitrary code. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	9.8	More Details
CVE-2020-28221	A CWE-20: Improper Input Validation vulnerability exists in EcoStruxure™ Operator Terminal Expert and Pro-face BLUE (version details in the notification) that could cause arbitrary code execution when the Ethernet Download feature is enable on the HMI.	9.8	More Details
CVE-2020-28998	An issue was discovered on Geeni GNC-CW013 doorbell 1.8.1 devices. A vulnerability exists in the Telnet service that allows a remote attacker to take full control of the device with a high-privileged account. The vulnerability exists because a system account has a default and static password.	9.8	More Details
CVE-2020-36199	TinyCheck before commits 9fd360d and ea53de8 was vulnerable to command injection due to insufficient checks of input parameters in several places.	9.8	More Details
CVE-2020-11213	Out of bound reads might occur in while processing Service descriptor due to improper validation of length of fields in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	9.8	More Details
CVE-2021-25900	An issue was discovered in the smallvec crate before 0.6.14 and 1.x before 1.6.1 for Rust. There is a heap-based buffer overflow in SmallVec::insert_many.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25907	An issue was discovered in the containers crate before 0.9.11 for Rust. When a panic occurs, a util::{mutate,mutate2} double drop can be performed.	9.8	More Details
CVE-2021-3185	A flaw was found in the gstreamer h264 component of gst-plugins-bad before v1.18.1 where when parsing a h264 header, an attacker could cause the stack to be smashed, memory corruption and possibly code execution.	9.8	More Details
CVE-2021-3188	phpList 3.6.0 allows CSV injection, related to the email parameter, and /lists/admin/ exports.	9.8	More Details
CVE-2021-3190	The async-git package before 1.13.2 for Node.js allows OS Command Injection via shell metacharacters, as demonstrated by git.reset and git.tag.	9.8	More Details
CVE-2021-3193	Improper access and command validation in the Nagios Docker Config Wizard before 1.1.2, as used in Nagios XI through 5.7, allows an unauthenticated attacker to execute remote code as the apache user.	9.8	More Details
CVE-2021-3199	Directory traversal with remote code execution can occur in /upload in ONLYOFFICE Document Server before 5.6.3, when JWT is used, via a /.. sequence in an image upload parameter.	9.8	More Details
CVE-2021-3278	Local Service Search Engine Management System 1.0 has a vulnerability through authentication bypass using SQL injection . Using this vulnerability, an attacker can bypass the login page.	9.8	More Details
CVE-2021-3286	SQL injection exists in Spotweb 1.4.9 because the notAllowedCommands protection mechanism is inadequate, e.g., a variation of the payload may be used. NOTE: this issue exists because of an incomplete fix for CVE-2020-35545.	9.8	More Details
CVE-2021-3304	Sagemcom F@ST 3686 v2 3.495 devices have a buffer overflow via a long sessionKey to the goform/login URI.	9.8	More Details
CVE-2020-27297	The affected product is vulnerable to a heap-based buffer overflow, which may allow an attacker to manipulate memory with controlled values and remotely execute code on the OPC UA Tunneller (versions prior to 6.3.0.8233).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11216	Buffer over read can happen in video driver when playing clip with atomsize having value UINT32_MAX in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	9.8	More Details
CVE-2020-11225	Out of bound access in WLAN driver due to lack of validation of array length before copying into array in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	9.8	More Details
CVE-2013-2512	The ftpd gem 0.2.1 for Ruby allows remote attackers to execute arbitrary OS commands via shell metacharacters in a LIST or NLST command argument within FTP protocol traffic.	9.8	More Details
CVE-2020-27221	In Eclipse OpenJ9 up to and including version 0.23, there is potential for a stack-based buffer overflow when the virtual machine or JNI natives are converting from UTF-8 characters to platform encoding.	9.8	More Details
CVE-2021-2108	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core Components). The supported version that is affected is 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 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-2021-1300	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	9.8	More Details
CVE-2021-2064	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core Components). The supported version that is affected is 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 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-2021-1301	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	9.8	More Details
CVE-2021-1138	Multiple vulnerabilities in the web UI of Cisco Smart Software Manager Satellite could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system. For more information about these vulnerabilities, see the Details section of this advisory.	9.8	More Details
CVE-2021-1139	Multiple vulnerabilities in the web UI of Cisco Smart Software Manager Satellite could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system. For more information about these vulnerabilities, see the Details section of this advisory.	9.8	More Details
CVE-2020-11212	Out of bounds reads while parsing NAN beacons attributes and OUIs due to improper length of field check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	9.8	More Details
CVE-2021-1140	Multiple vulnerabilities in the web UI of Cisco Smart Software Manager Satellite could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system. For more information about these vulnerabilities, see the Details section of this advisory.	9.8	More Details
CVE-2021-1141	Multiple vulnerabilities in the web UI of Cisco Smart Software Manager Satellite could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system. For more information about these vulnerabilities, see the Details section of this advisory.	9.8	More Details
CVE-2021-1142	Multiple vulnerabilities in the web UI of Cisco Smart Software Manager Satellite could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system. For more information about these vulnerabilities, see the Details section of this advisory.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2047	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 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-2020-11136	Buffer Over-read in audio driver while using malloc management function due to not returning NULL for zero sized memory requirement in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	9.8	More Details
CVE-2020-11137	Integer multiplication overflow resulting in lower buffer size allocation than expected causes memory access out of bounds resulting in possible device instability in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	9.8	More Details
CVE-2020-11138	Uninitialized pointers accessed during music play back with incorrect bit stream due to an uninitialized heap memory result in instability in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	9.8	More Details
CVE-2020-11140	Out of bound memory access during music playback with ALAC modified content due to improper validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	9.8	More Details
CVE-2021-2029	Vulnerability in the Oracle Scripting product of Oracle E-Business Suite (component: Miscellaneous). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Scripting. Successful attacks of this vulnerability can result in takeover of Oracle Scripting. 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-2021-1994	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 and 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in 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-2020-11143	Out of bound memory access during music playback with modified content due to copying data without checking destination buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	9.8	More Details
CVE-2020-11167	Memory corruption while calculating L2CAP packet length in reassembly logic when remote sends more data than expected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	9.8	More Details
CVE-2020-11197	Possible integer overflow can occur when stream info update is called when total number of streams detected are zero while parsing TS clip with invalid data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	9.8	More Details
CVE-2021-2075	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Samples). 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 IIOP, T3 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-2021-1264	A vulnerability in the Command Runner tool of Cisco DNA Center could allow an authenticated, remote attacker to perform a command injection attack. The vulnerability is due to insufficient input validation by the Command Runner tool. An attacker could exploit this vulnerability by providing crafted input during command execution or via a crafted command runner API call. A successful exploit could allow the attacker to execute arbitrary CLI commands on devices managed by Cisco DNA Center.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2100	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Print Server). 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 One-to-One Fulfillment. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle One-to-One Fulfillment accessible data as well as unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment 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-2020-27299	The affected product is vulnerable to an out-of-bounds read, which may allow an attacker to obtain and disclose sensitive data information or cause the device to crash on the OPC UA Tunneller (versions prior to 6.3.0.8233).	9.1	More Details
CVE-2020-11215	An out of bounds read can happen when processing VSA attribute due to improper minimum required length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	9.1	More Details
CVE-2021-2101	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Print Server). 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 One-to-One Fulfillment. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle One-to-One Fulfillment accessible data as well as unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment 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 Number	Description	Base Score	Reference
CVE-2021-25905	An issue was discovered in the bra crate before 0.1.1 for Rust. It lacks soundness because it can read uninitialized memory.	9.1	More Details
CVE-2021-1225	Multiple vulnerabilities in the web-based management interface of Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to conduct SQL injection attacks on an affected system. These vulnerabilities exist because the web-based management interface improperly validates values in SQL queries. An attacker could exploit these vulnerabilities by authenticating to the application and sending malicious SQL queries to an affected system. A successful exploit could allow the attacker to modify values on or return values from the underlying database or the operating system.	9.1	More Details
CVE-2021-23901	An XML external entity (XXE) injection vulnerability was discovered in the Nutch DmozParser and is known to affect Nutch versions < 1.18. XML external entity injection (also known as XXE) is a web security vulnerability that allows an attacker to interfere with an application's processing of XML data. It often allows an attacker to view files on the application server filesystem, and to interact with any back-end or external systems that the application itself can access. This issue is fixed in Apache Nutch 1.18.	9.1	More Details
CVE-2020-8570	Kubernetes Java client libraries in version 10.0.0 and versions prior to 9.0.1 allow writes to paths outside of the current directory when copying multiple files from a remote pod which sends a maliciously crafted archive. This can potentially overwrite any files on the system of the process executing the client code.	9.1	More Details
CVE-2020-11144	Buffer over-read while UE process invalid DL ROHC packet for decompression due to lack of check of size of compresses packet in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	9.1	More Details
CVE-2020-35270	Student Result Management System In PHP With Source Code is affected by SQL injection. An attacker can able to access of Admin Panel and manage every account of Result.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference

CVE Number	Description	Base Score	Reference
CVE-2021-3317	KLog Server through 2.4.1 allows authenticated command injection. async.php calls shell_exec() on the original value of the source parameter.	8.8	More Details
CVE-2020-4921	IBM Security Guardium 10.6 and 11.2 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 191398.	8.8	More Details
CVE-2020-35576	A Command Injection issue in the traceroute feature on TP-Link TL-WR841N V13 (JP) with firmware versions prior to 201216 allows authenticated users to execute arbitrary code as root via shell metacharacters, a different vulnerability than CVE-2018-12577.	8.8	More Details
CVE-2020-35239	A vulnerability exists in CakePHP versions 4.0.x through 4.1.3. The CsrfProtectionMiddleware component allows method override parameters to bypass CSRF checks by changing the HTTP request method to an arbitrary string that is not in the list of request methods that CakePHP checks. Additionally, the route middleware does not verify that this overriden method (which can be an arbitrary string) is actually an HTTP method.	8.8	More Details
CVE-2020-24549	openMAINT before 1.1-2.4.2 allows remote authenticated users to run arbitrary JSP code on the underlying web server.	8.8	More Details
CVE-2021-25863	Open5GS 2.1.3 listens on 0.0.0.0:3000 and has a default password of 1423 for the admin account.	8.8	More Details
CVE-2020-23826	The Yale WIPC-303W 2.21 through 2.31 camera is vulnerable to remote command execution (RCE) through command injection via the HTTP API. NOTE: This may be a duplicate of CVE-2020-10176	8.8	More Details
CVE-2021-1272	A vulnerability in the session validation feature of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to bypass access controls and conduct a server-side request forgery (SSRF) attack on a targeted system. This vulnerability is due to insufficient validation of parameters in a specific HTTP request by an attacker. An attacker could exploit this vulnerability by sending a crafted HTTP request to an authenticated user of the DCNM web application. A successful exploit could allow the attacker to bypass access controls and gain unauthorized access to the Device Manager application, which provides access to network devices managed by the system.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-23160	Remote code execution in Pyrescom Termod4 time management devices before 10.04k allows authenticated remote attackers to arbitrary commands as root on the devices.	8.8	More Details
CVE-2020-17532	When handler-router component is enabled in servicecomb-java-chassis, authenticated user may inject some data and cause arbitrary code execution. The problem happens in versions between 2.0.0 ~ 2.1.3 and fixed in Apache ServiceComb-Java-Chassis 2.1.5	8.8	More Details
CVE-2020-12511	Pepperl+Fuchs Comtrol IO-Link Master in Version 1.5.48 and below is prone to a Cross-Site Request Forgery (CSRF) in the web interface.	8.8	More Details
CVE-2021-22847	Hyweb HyCMS-J1's API fail to filter POST request parameters. Remote attackers can inject SQL syntax and execute commands without privilege.	8.8	More Details
CVE-2021-3164	ChurchRota 2.6.4 is vulnerable to authenticated remote code execution. The user does not need to have file upload permission in order to upload and execute an arbitrary file via a POST request to resources.php.	8.8	More Details
CVE-2020-9492	In Apache Hadoop 3.2.0 to 3.2.1, 3.0.0-alpha1 to 3.1.3, and 2.0.0-alpha to 2.10.0, WebHDFS client might send SPNEGO authorization header to remote URL without proper verification.	8.8	More Details
CVE-2021-1247	Multiple vulnerabilities in certain REST API endpoints of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to execute arbitrary SQL commands on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	8.8	More Details
CVE-2021-1248	Multiple vulnerabilities in certain REST API endpoints of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to execute arbitrary SQL commands on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	8.8	More Details
CVE-2021-1298	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1302	Multiple vulnerabilities in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization and modify the configuration of an affected system, gain access to sensitive information, and view information that they are not authorized to access. For more information about these vulnerabilities, see the Details section of this advisory.	8.8	More Details
CVE-2021-3165	SmartAgent 3.1.0 allows a ViewOnly attacker to create a SuperUser account via the /#/CampaignManager/users URI.	8.8	More Details
CVE-2020-19364	OpenEMR 5.0.1 allows an authenticated attacker to upload and execute malicious PHP scripts through /controller.php.	8.8	More Details
CVE-2021-1257	A vulnerability in the web-based management interface of Cisco DNA Center Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack to manipulate an authenticated user into executing malicious actions without their awareness or consent. The vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a web-based management user to follow a specially crafted link. A successful exploit could allow the attacker to perform arbitrary actions on the device with the privileges of the authenticated user. These actions include modifying the device configuration, disconnecting the user's session, and executing Command Runner commands.	8.8	More Details
CVE-2021-1305	Multiple vulnerabilities in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization and modify the configuration of an affected system, gain access to sensitive information, and view information that they are not authorized to access. For more information about these vulnerabilities, see the Details section of this advisory.	8.8	More Details
CVE-2021-1299	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2035	Vulnerability in the RDBMS Scheduler component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows low privileged attacker having Export Full Database privilege with network access via Oracle Net to compromise RDBMS Scheduler. Successful attacks of this vulnerability can result in takeover of RDBMS Scheduler. 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-2021-1303	A vulnerability in the user management roles of Cisco DNA Center could allow an authenticated, remote attacker to execute unauthorized commands on an affected device. The vulnerability is due to improper enforcement of actions for assigned user roles. An attacker could exploit this vulnerability by authenticating as a user with an Observer role and executing commands on the affected device. A successful exploit could allow a user with the Observer role to execute commands to view diagnostic information of the devices that Cisco DNA Center manages.	8.8	More Details
CVE-2020-35217	Vert.x-Web framework v4.0 milestone 1-4 does not perform a correct CSRF verification. Instead of comparing the CSRF token in the request with the CSRF token in the cookie, it compares the CSRF token in the cookie against a CSRF token that is stored in the session. An attacker does not even need to provide a CSRF token in the request because the framework does not consider it. The cookies are automatically sent by the browser and the verification will always succeed, leading to a successful CSRF attack.	8.8	More Details
CVE-2021-1304	Multiple vulnerabilities in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization and modify the configuration of an affected system, gain access to sensitive information, and view information that they are not authorized to access. For more information about these vulnerabilities, see the Details section of this advisory.	8.8	More Details
CVE-2020-26295	OpenMage is a community-driven alternative to Magento CE. In OpenMage before versions 19.4.10 and 20.0.5, an administrator with permission to import/export data and to edit cms pages was able to inject an executable file on the server via layout xml. The latest OpenMage Versions up from 19.4.9 and 20.0.5 have this Issue solved	8.7	More Details
CVE-2020-26285	OpenMage is a community-driven alternative to Magento CE. In OpenMage before versions 19.4.10 and 20.0.5, there is a vulnerability which enables remote code execution. In affected versions an administrator with permission to import/export data and to create widget instances was able to inject an executable file on the server. The latest OpenMage Versions up from 19.4.9 and 20.0.5 have this Issue solved	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26252	OpenMage is a community-driven alternative to Magento CE. In OpenMage before versions 19.4.10 and 20.0.6, there is a vulnerability which enables remote code execution. In affected versions an administrator with permission to update product data to be able to store an executable file on the server and load it via layout xml. The latest OpenMage Versions up from 19.4.10 and 20.0.6 have this issue solved.	8.7	More Details
CVE-2021-1279	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	8.6	More Details
CVE-2021-2068	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). Supported versions that are affected are 8.5.4 and 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 creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L).	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2067	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). Supported versions that are affected are 8.5.4 and 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 creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L).	8.6	More Details
CVE-2021-2066	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). Supported versions that are affected are 8.5.4 and 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 creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L).	8.6	More Details
CVE-2021-1278	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1274	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	8.6	More Details
CVE-2021-1241	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	8.6	More Details
CVE-2021-2069	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). Supported versions that are affected are 8.5.4 and 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 creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L).	8.6	More Details
CVE-2021-1273	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	8.6	More Details
CVE-2021-21278	RSSHub is an open source, easy to use, and extensible RSS feed generator. In RSSHub before version 7f1c430 (non-semantic versioning) there is a risk of code injection. Some routes use `eval` or `Function constructor`, which may be injected by the target site with unsafe code, causing server-side security issues The fix in version 7f1c430 is to temporarily remove the problematic route and added a `no-new-func` rule to eslint.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2063	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where PeopleSoft Enterprise PeopleTools executes to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 8.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	8.4	More Details
CVE-2021-2018	Vulnerability in the Advanced Networking Option component of Oracle Database Server. Supported versions that are affected are 18c 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: CVE-2021-2018 affects Windows platform only. 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-2021-2084	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, 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 CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation 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-2021-2091	Vulnerability in the Oracle Scripting product of Oracle E-Business Suite (component: Miscellaneous). 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 Scripting. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Scripting, 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 Scripting accessible data as well as unauthorized update, insert or delete access to some of Oracle Scripting 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-2021-2090	Vulnerability in the Oracle Email Center product of Oracle E-Business Suite (component: Message Display). 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 Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, 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 Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center 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-2020-4949	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 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: 192025.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2085	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, 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 CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation 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-2021-2082	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). 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 iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, 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 iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore 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-2021-2083	Vulnerability in the Oracle iSupport product of Oracle E-Business Suite (component: User Responsibilities). 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 iSupport. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iSupport, 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 iSupport accessible data as well as unauthorized update, insert or delete access to some of Oracle iSupport 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-2021-2093	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-2021-2080	Vulnerability in the Oracle Configurator product of Oracle Supply Chain (component: UI Servlet). Supported versions that are affected are 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Configurator. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Configurator, 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 Configurator accessible data as well as unauthorized update, insert or delete access to some of Oracle Configurator 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-2021-2079	Vulnerability in the Oracle Configurator product of Oracle Supply Chain (component: UI Servlet). Supported versions that are affected are 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Configurator. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Configurator, 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 Configurator accessible data as well as unauthorized update, insert or delete access to some of Oracle Configurator 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-2021-2078	Vulnerability in the Oracle Configurator product of Oracle Supply Chain (component: UI Servlet). Supported versions that are affected are 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Configurator. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Configurator, 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 Configurator accessible data as well as unauthorized update, insert or delete access to some of Oracle Configurator 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-2021-2077	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). 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 iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, 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 iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore 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-2021-2092	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, 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 CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation 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-2021-2096	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). 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 iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, 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 iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore 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-2021-2094	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Print Server). 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 One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, 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 One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment 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-2021-2097	Vulnerability in the Oracle iSupport product of Oracle E-Business Suite (component: Profile). 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 iSupport. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iSupport, 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 iSupport accessible data as well as unauthorized update, insert or delete access to some of Oracle iSupport 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-2021-2098	Vulnerability in the Oracle Email Center product of Oracle E-Business Suite (component: Message Display). 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 Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, 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 Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center 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-2021-2099	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, 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 CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation 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-2021-2102	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle Supply Chain (component: Dialog Box). Supported versions that are affected are 11.5.10, 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Complex Maintenance, Repair, and Overhaul, 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 Complex Maintenance, Repair, and Overhaul accessible data as well as unauthorized update, insert or delete access to some of Oracle Complex Maintenance, Repair, and Overhaul 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-2021-2103	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle Supply Chain (component: Dialog Box). Supported versions that are affected are 11.5.10, 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Complex Maintenance, Repair, and Overhaul, 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 Complex Maintenance, Repair, and Overhaul accessible data as well as unauthorized update, insert or delete access to some of Oracle Complex Maintenance, Repair, and Overhaul 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-2021-2104	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle Supply Chain (component: Dialog Box). Supported versions that are affected are 11.5.10, 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Complex Maintenance, Repair, and Overhaul, 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 Complex Maintenance, Repair, and Overhaul accessible data as well as unauthorized update, insert or delete access to some of Oracle Complex Maintenance, Repair, and Overhaul 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-2021-2105	Vulnerability in the Oracle Customer Interaction History product of Oracle E-Business Suite (component: Outcome-Result). 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 Customer Interaction History. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Customer Interaction History, 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 Customer Interaction History accessible data as well as unauthorized update, insert or delete access to some of Oracle Customer Interaction History 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-2021-2106	Vulnerability in the Oracle Customer Interaction History product of Oracle E-Business Suite (component: Outcome-Result). 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 Customer Interaction History. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Customer Interaction History, 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 Customer Interaction History accessible data as well as unauthorized update, insert or delete access to some of Oracle Customer Interaction History 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-2021-2107	Vulnerability in the Oracle Customer Interaction History product of Oracle E-Business Suite (component: Outcome-Result). 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 Customer Interaction History. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Customer Interaction History, 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 Customer Interaction History accessible data as well as unauthorized update, insert or delete access to some of Oracle Customer Interaction History 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-2021-2114	Vulnerability in the Oracle Common Applications Calendar product of Oracle E-Business Suite (component: Applications Calendar). 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 Calendar. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Applications Calendar, 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 Calendar accessible data as well as unauthorized update, insert or delete access to some of Oracle Common Applications Calendar 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-2021-2118	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-2021-2074	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. 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 Number	Description	Base Score	Reference
CVE-2021-2015	Vulnerability in the Oracle Workflow product of Oracle E-Business Suite (component: Worklist). Supported versions that are affected are 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Workflow. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Workflow, 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 Workflow accessible data as well as unauthorized update, insert or delete access to some of Oracle Workflow 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-2021-2089	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Runtime Catalog). 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 iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, 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 iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore 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-2021-2034	Vulnerability in the Oracle Common Applications Calendar product of Oracle E-Business Suite (component: Tasks). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Common Applications Calendar. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Applications Calendar, 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 Calendar accessible data as well as unauthorized update, insert or delete access to some of Oracle Common Applications Calendar 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-2021-2025	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web General). Supported versions that are affected are 5.5.0.0.0, 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 Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition 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-2021-2026	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-2021-2027	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 Number	Description	Base Score	Reference
CVE-2021-1222	A vulnerability in the web-based management interface of Cisco Smart Software Manager Satellite could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. The vulnerability exists because the web-based management interface improperly validates values within SQL queries. An attacker could exploit this vulnerability by authenticating to the application and sending malicious SQL queries to an affected system. A successful exploit could allow the attacker to modify values on or return values from the underlying database or the operating system.	8.1	More Details
CVE-2020-25682	A flaw was found in dnsmasq before 2.83. A buffer overflow vulnerability was discovered in the way dnsmasq extract names from DNS packets before validating them with DNSSEC data. An attacker on the network, who can create valid DNS replies, could use this flaw to cause an overflow with arbitrary data in a heap-allocated memory, possibly executing code on the machine. The flaw is in the rfc1035.c:extract_name() function, which writes data to the memory pointed by name assuming MAXDNAME*2 bytes are available in the buffer. However, in some code execution paths, it is possible extract_name() gets passed an offset from the base buffer, thus reducing, in practice, the number of available bytes that can be written in the buffer. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	8.1	More Details
CVE-2021-2041	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Installation). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Difficult to exploit 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 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-2021-2071	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Elastic Search). Supported versions that are affected are 8.56, 8.57 and 8.58. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. 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 Number	Description	Base Score	Reference
CVE-2021-3309	packages/wekan-ldap/server/ldap.js in Wekan before 4.87 can process connections even though they are not authorized by the Certification Authority trust store,	8.1	More Details
CVE-2021-1997	Vulnerability in the Oracle Hospitality Reporting and Analytics product of Oracle Food and Beverage Applications (component: Report). 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-2020-25681	A flaw was found in dnsmasq before version 2.83. A heap-based buffer overflow was discovered in the way RRSets are sorted before validating with DNSSEC data. An attacker on the network, who can forge DNS replies such as that they are accepted as valid, could use this flaw to cause a buffer overflow with arbitrary data in a heap memory segment, possibly executing code on the machine. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	8.1	More Details
CVE-2021-2129	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. 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 creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data as well as unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N).	7.9	More Details
CVE-2020-11146	Out of bound write while copying data using IOCTL due to lack of check of array index received from user in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11180	Out of bound access in computer vision control due to improper validation of command length before processing it in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	7.8	More Details
CVE-2020-35845	FastStone Image Viewer 7.5 has an out-of-bounds write (via a crafted image file) at FSViewer.exe+0x96cf.	7.8	More Details
CVE-2020-14360	A flaw was found in the X.Org Server before version 1.20.10. An out-of-bounds access in the XkbSetMap function may lead to a privilege escalation vulnerability. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.8	More Details
CVE-2021-1068	NVIDIA SHIELD TV, all versions prior to 8.2.2, contains a vulnerability in the NVDEC component, in which an attacker can read from or write to a memory location that is outside the intended boundary of the buffer, which may lead to denial of service or escalation of privileges.	7.8	More Details
CVE-2021-26025	PlugIns\IDE_ACDStd.apl in ACDSee Professional 2021 14.0 1721 has a User Mode Write Access Violation starting at IDE_ACDStd!zlibVersion+0x0000000000004e5e via a crafted BMP image.	7.8	More Details
CVE-2020-36210	An issue was discovered in the autorand crate before 0.2.3 for Rust. Because of impl Random on arrays, uninitialized memory can be dropped when a panic occurs, leading to memory corruption.	7.8	More Details
CVE-2020-4983	IBM Spectrum LSF 10.1 and IBM Spectrum LSF Suite 10.2 could allow a user on the local network who has privileges to submit LSF jobs to execute arbitrary commands. IBM X-Force ID: 192586.	7.8	More Details
CVE-2020-11181	Out of bound access issue while handling cvp process control command due to improper validation of buffer pointer received from HLOS in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	7.8	More Details
CVE-2020-36208	An issue was discovered in the conquer-once crate before 0.3.2 for Rust. Thread crossing can occur for a non-Send but Sync type, leading to memory corruption.	7.8	More Details
CVE-2020-11185	Out of bound issue in WLAN driver while processing vdev responses from firmware due to lack of validation of data received from firmware in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11217	A possible double free or invalid memory access in audio driver while reading Speaker Protection parameters in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	7.8	More Details
CVE-2021-1219	A vulnerability in Cisco Smart Software Manager Satellite could allow an authenticated, local attacker to access sensitive information on an affected system. The vulnerability is due to insufficient protection of static credentials in the affected software. An attacker could exploit this vulnerability by gaining access to the static credential that is stored on the local device. A successful exploit could allow the attacker to view static credentials, which the attacker could use to carry out further attacks.	7.8	More Details
CVE-2020-35844	FastStone Image Viewer 7.5 has an out-of-bounds write (via a crafted image file) at FSViewer.exe+0xbe9c4.	7.8	More Details
CVE-2021-1261	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory.	7.8	More Details
CVE-2021-22697	A CWE-434: Unrestricted Upload of File with Dangerous Type vulnerability exists in the EcoStruxure Power Build - Rapsody software (V2.1.13 and prior) that could allow a use-after-free condition which could result in remote code execution when a malicious SSD file is uploaded and improperly parsed.	7.8	More Details
CVE-2020-27814	A heap-buffer overflow was found in the way openjpeg2 handled certain PNG format files. An attacker could use this flaw to cause an application crash or in some cases execute arbitrary code with the permission of the user running such an application.	7.8	More Details
CVE-2021-1263	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory.	7.8	More Details
CVE-2020-27288	An untrusted pointer dereference has been identified in the way TPEditor(v1.98 and prior) processes project files, allowing an attacker to craft a special project file that may permit arbitrary code execution.	7.8	More Details
CVE-2020-27284	TPEditor (v1.98 and prior) is vulnerable to two out-of-bounds write instances in the way it processes project files, allowing an attacker to craft a special project file that may permit arbitrary code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27280	A use after free issue has been identified in the way ISPSoft(v3.12 and prior) processes project files, allowing an attacker to craft a special project file that may allow arbitrary code execution.	7.8	More Details
CVE-2020-25737	An elevation of privilege vulnerability exists in Hackolade versions prior 4.2.0 on Windows has an issue in specific deployment scenarios that could allow local users to gain elevated privileges during an uninstall of the application.	7.8	More Details
CVE-2020-25173	An attacker with local network access can obtain a fixed cryptography key which may allow for further compromise of Reolink P2P cameras outside of local network access	7.8	More Details
CVE-2021-1262	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory.	7.8	More Details
CVE-2021-22698	A CWE-434: Unrestricted Upload of File with Dangerous Type vulnerability exists in the EcoStruxure Power Build - Rapsody software (V2.1.13 and prior) that could allow a stack-based buffer overflow to occur which could result in remote code execution when a malicious SSD file is uploaded and improperly parsed.	7.8	More Details
CVE-2021-26026	PlugIns\IDE_ACDStd.apl in ACDSee Professional 2021 14.0 1721 has a User Mode Write Access Violation starting at IDE_ACDStd!JPEGTransW+0x000000000000c7f4 via a crafted BMP image.	7.8	More Details
CVE-2021-1260	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory.	7.8	More Details
CVE-2021-3156	Sudo before 1.9.5p2 contains an off-by-one error that can result in a heap-based buffer overflow, which allows privilege escalation to root via "sudoedit -s" and a command-line argument that ends with a single backslash character.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1280	A vulnerability in the loading mechanism of specific DLLs of Cisco Advanced Malware Protection (AMP) for Endpoints for Windows and Immunet for Windows could allow an authenticated, local attacker to perform a DLL hijacking attack. To exploit this vulnerability, the attacker would need valid credentials on the Windows system. This vulnerability is due to incorrect handling of directory search paths at run time. An attacker could exploit this vulnerability by placing a malicious DLL file on the targeted system. This file will execute when the vulnerable application launches. A successful exploit could allow the attacker to execute arbitrary code on the targeted system with SYSTEM privileges.	7.8	More Details
CVE-2021-22159	Insider Threat Management Windows Agent Local Privilege Escalation Vulnerability The Proofpoint Insider Threat Management (formerly ObserveIT) Agent for Windows before 7.4.3, 7.5.4, 7.6.5, 7.7.5, 7.8.4, 7.9.3, 7.10.2, and 7.11.0.25 as well as versions 7.3 and earlier is missing authentication for a critical function, which allows a local authenticated Windows user to run arbitrary commands with the privileges of the Windows SYSTEM user. Agents for MacOS, Linux, and ITM Cloud are not affected.	7.8	More Details
CVE-2020-6024	Check Point SmartConsole before R80.10 Build 185, R80.20 Build 119, R80.30 before Build 94, R80.40 before Build 415, and R81 before Build 548 were vulnerable to a possible local privilege escalation due to running executables from a directory with write access to all authenticated users.	7.8	More Details
CVE-2021-3297	On Zyxel NBG2105 V1.00(AAGU.2)C0 devices, setting the login cookie to 1 provides administrator access.	7.8	More Details
CVE-2020-4688	IBM Security Guardium 10.6 and 11.2 could allow a local attacker to execute arbitrary commands on the system as an unprivileged user, caused by command injection vulnerability. IBM X-Force ID: 186700.	7.8	More Details
CVE-2020-16236	FPWIN Pro is vulnerable to an out-of-bounds read vulnerability when a user opens a maliciously crafted project file, which may allow an attacker to remotely execute arbitrary code.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21272	ORAS is open source software which enables a way to push OCI Artifacts to OCI Conformant registries. ORAS is both a CLI for initial testing and a Go Module. In ORAS from version 0.4.0 and before version 0.9.0, there is a "zip-slip" vulnerability. The directory support feature allows the downloaded gzipped tarballs to be automatically extracted to the user-specified directory where the tarball can have symbolic links and hard links. A well-crafted tarball or tarballs allow malicious artifact providers linking, writing, or overwriting specific files on the host filesystem outside of the user-specified directory unexpectedly with the same permissions as the user who runs `oras pull`. Users of the affected versions are impacted if they are `oras` CLI users who runs `oras pull`, or if they are Go programs, which invoke `github.com/deislabs/oras/pkg/content.FileStore`. The problem has been fixed in version 0.9.0. For `oras` CLI users, there is no workarounds other than pulling from a trusted artifact provider. For `oras` package users, the workaround is to not use `github.com/deislabs/oras/pkg/content.FileStore`, and use other content stores instead, or pull from a trusted artifact provider.	7.7	More Details
CVE-2021-21269	Keymaker is a Mastodon Community Finder based Matrix Community serverlist page Server. In Keymaker before version 0.2.0, the assets endpoint did not check for the extension. The rust `join` method without checking user input might have made it abe to do a Path Traversal attack causing to read more files than allowed. This is fixed in version 0.2.0.	7.7	More Details
CVE-2021-2115	Vulnerability in the Oracle Common Applications Calendar product of Oracle E-Business Suite (component: Tasks). 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 Common Applications Calendar. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Applications Calendar, 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 Calendar accessible data as well as unauthorized update, insert or delete access to some of Oracle Common Applications Calendar 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-2021-21260	Online Invoicing System (OIS) is open source software which is a lean invoicing system for small businesses, consultants and freelancers created using AppGini. In OIS version 4.0 there is a stored XSS which can enables an attacker takeover of the admin account through a payload that extracts a csrf token and sends a request to change password. It has been found that Item description is reflected without sanitization in app/items_view.php which enables the malicious scenario.	7.6	More Details
CVE-2021-2051	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 unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data as well as unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle BI Publisher. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L).	7.6	More Details
CVE-2021-2050	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 unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data as well as unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle BI Publisher. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L).	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2039	Vulnerability in the Siebel Core - Server Framework product of Oracle Siebel CRM (component: Search). Supported versions that are affected are 20.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel Core - Server Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Siebel Core - Server 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 Siebel Core - Server Framework accessible data as well as unauthorized update, insert or delete access to some of Siebel Core - Server 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-2021-2062	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Web Server). 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 require human interaction from a person other than the attacker and while the vulnerability is in Oracle BI Publisher, 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 BI Publisher accessible data as well as unauthorized update, insert or delete access to some of Oracle BI Publisher 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-2021-2049	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Administration). 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 unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data as well as unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle BI Publisher. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L).	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2013	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 unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data as well as unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle BI Publisher. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L).	7.6	More Details
CVE-2020-27295	The affected product has uncontrolled resource consumption issues, which may allow an attacker to cause a denial-of-service condition on the OPC UA Tunneller (versions prior to 6.3.0.8233).	7.5	More Details
CVE-2020-0236	In A2DP_GetCodecType of a2dp_codec_config, there is a possible out-of-bounds read due to improper input validation. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android, Versions: Android-10, Android ID: A-79703353.	7.5	More Details
CVE-2021-21723	Some ZTE products have a DoS vulnerability. Due to the improper handling of memory release in some specific scenarios, a remote attacker can trigger the vulnerability by performing a series of operations, resulting in memory leak, which may eventually lead to device denial of service. This affects: ZXR10 9904, ZXR10 9908, ZXR10 9916, ZXR10 9904-S, ZXR10 9908-S; all versions up to V1.01.10.B12.	7.5	More Details
CVE-2020-28874	reset-password.php in ProjectSend before r1295 allows remote attackers to reset a password because of incorrect business logic. Errors are not properly considered (an invalid token parameter).	7.5	More Details
CVE-2021-25908	An issue was discovered in the fil-ocl crate through 2021-01-04 for Rust. From<EventList> can lead to a double free.	7.5	More Details
CVE-2020-23162	Sensitive information disclosure and weak encryption in Pyrescom Termod4 time management devices before 10.04k allows remote attackers to read a session-file and obtain plain-text user credentials.	7.5	More Details
CVE-2020-13582	A denial-of-service vulnerability exists in the HTTP Server functionality of Micrium uC-HTTP 3.01.00. A specially crafted HTTP request can lead to denial of service. An attacker can send an HTTP request to trigger this vulnerability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27274	Some parsing functions in the affected product do not check the return value of malloc and the thread handling the message is forced to close, which may lead to a denial-of-service condition on the OPC UA Tunneller (versions prior to 6.3.0.8233).	7.5	More Details
CVE-2020-23449	newbee-mall all versions are affected by incorrect access control to remotely gain privileges through NewBeeMallIndexConfigServiceImpl.java. Unauthorized changes can be made to any user information through the userID.	7.5	More Details
CVE-2021-25906	An issue was discovered in the basic_dsp_matrix crate before 0.9.2 for Rust. When a TransformContent panic occurs, a double drop can be performed.	7.5	More Details
CVE-2021-25904	An issue was discovered in the av-data crate before 0.3.0 for Rust. A raw pointer is dereferenced, leading to a read of an arbitrary memory address, sometimes causing a segfault.	7.5	More Details
CVE-2021-3223	Node-RED-Dashboard before 2.26.2 allows ui_base/js/..%2f directory traversal to read files.	7.5	More Details
CVE-2021-25903	An issue was discovered in the cache crate through 2021-01-01 for Rust. A raw pointer is dereferenced.	7.5	More Details
CVE-2020-36230	A flaw was discovered in OpenLDAP before 2.4.57 leading in an assertion failure in slapd in the X.509 DN parsing in decode.c ber_next_element, resulting in denial of service.	7.5	More Details
CVE-2021-25902	An issue was discovered in the glsl-layout crate before 0.4.0 for Rust. When a panic occurs, map_array can perform a double drop.	7.5	More Details
CVE-2021-1277	Multiple vulnerabilities in Cisco Data Center Network Manager (DCNM) could allow an attacker to spoof a trusted host or construct a man-in-the-middle attack to extract sensitive information or alter certain API requests. These vulnerabilities are due to insufficient certificate validation when establishing HTTPS requests with the affected device. For more information about these vulnerabilities, see the Details section of this advisory.	7.5	More Details
CVE-2021-25864	node-red-contrib-huemagic 3.0.0 is affected by hue/assets/..%2F Directory Traversal.in the res.sendFile API, used in file hue-magic.js, to fetch an arbitrary file.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1276	Multiple vulnerabilities in Cisco Data Center Network Manager (DCNM) could allow an attacker to spoof a trusted host or construct a man-in-the-middle attack to extract sensitive information or alter certain API requests. These vulnerabilities are due to insufficient certificate validation when establishing HTTPS requests with the affected device. For more information about these vulnerabilities, see the Details section of this advisory.	7.5	More Details
CVE-2020-25169	The affected Reolink P2P products do not sufficiently protect data transferred between the local device and Reolink servers. This can allow an attacker to access sensitive information, such as camera feeds.	7.5	More Details
CVE-2020-27541	Denial of Service vulnerability in Rostelecom CS-C2SHW 5.0.082.1. AgentGreen service has a bug in parsing broadcast discovery UDP packet. Sending a packet of too small size will lead to an attempt of allocating buffer of negative size. As the result service AgentGreen will be terminated and started again later.	7.5	More Details
CVE-2020-23776	A SSRF vulnerability exists in Winmail 6.5 in app.php in the key parameter when HTTPS is on. An attacker can use this vulnerability to cause the server to send a request to a specific URL. An attacker can modify the request header 'HOST' value to cause the server to send the request.	7.5	More Details
CVE-2020-36201	An issue was discovered in certain Xerox WorkCentre products. They do not properly encrypt passwords. This affects 3655, 3655i, 58XX, 58XXi 59XX, 59XXi, 6655, 6655i, 72XX, 72XXi 78XX, 78XXi, 7970, 7970i, EC7836, and EC7856 devices.	7.5	More Details
CVE-2020-12512	Pepperl+Fuchs Comtrol IO-Link Master in Version 1.5.48 and below is prone to an authenticated reflected POST Cross-Site Scripting	7.5	More Details
CVE-2020-36227	A flaw was discovered in OpenLDAP before 2.4.57 leading to an infinite loop in slapd with the cancel_extop Cancel operation, resulting in denial of service.	7.5	More Details
CVE-2020-11214	Buffer over-read while processing NDL attribute if attribute length is larger than expected and then FW is treating it as more number of immutable schedules in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36226	A flaw was discovered in OpenLDAP before 2.4.57 leading to a memch->bv_len miscalculation and slapd crash in the saslAuthzTo processing, resulting in denial of service.	7.5	More Details
CVE-2020-4766	IBM MQ Internet Pass-Thru 2.1 and 9.2 could allow a remote user to cause a denial of service by sending malformed MQ data requests which would consume all available resources. IBM X-Force ID: 188093.	7.5	More Details
CVE-2020-36228	An integer underflow was discovered in OpenLDAP before 2.4.57 leading to a slapd crash in the Certificate List Exact Assertion processing, resulting in denial of service.	7.5	More Details
CVE-2020-36225	A flaw was discovered in OpenLDAP before 2.4.57 leading to a double free and slapd crash in the saslAuthzTo processing, resulting in denial of service.	7.5	More Details
CVE-2021-26266	cPanel before 92.0.9 allows a Reseller to bypass the suspension lock (SEC-578).	7.5	More Details
CVE-2021-26267	cPanel before 92.0.9 allows a MySQL user (who has an old-style password hash) to bypass suspension (SEC-579).	7.5	More Details
CVE-2020-36229	A flaw was discovered in ldap_X509dn2bv in OpenLDAP before 2.4.57 leading to a slapd crash in the X.509 DN parsing in ad_keystring, resulting in denial of service.	7.5	More Details
CVE-2020-36224	A flaw was discovered in OpenLDAP before 2.4.57 leading to an invalid pointer free and slapd crash in the saslAuthzTo processing, resulting in denial of service.	7.5	More Details
CVE-2020-3685	Pointer variable which is freed is not cleared can result in memory corruption and leads to denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2020-36223	A flaw was discovered in OpenLDAP before 2.4.57 leading to a slapd crash in the Values Return Filter control handling, resulting in denial of service (double free and out-of-bounds read).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11200	Buffer over-read while parsing RPS due to lack of check of input validation on values received from user side. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	7.5	More Details
CVE-2021-3195	bitcoind in Bitcoin Core through 0.21.0 can create a new file in an arbitrary directory (e.g., outside the ~/.bitcoin directory) via a dumpwallet RPC call. NOTE: this reportedly does not violate the security model of Bitcoin Core, but can violate the security model of a fork that has implemented dumpwallet restrictions	7.5	More Details
CVE-2020-36222	A flaw was discovered in OpenLDAP before 2.4.57 leading to an assertion failure in slapd in the saslAuthzTo validation, resulting in denial of service.	7.5	More Details
CVE-2020-36221	An integer underflow was discovered in OpenLDAP before 2.4.57 leading to slapd crashes in the Certificate Exact Assertion processing, resulting in denial of service (schema_init.c serialNumberAndIssuerCheck).	7.5	More Details
CVE-2020-36215	An issue was discovered in the hashconsing crate before 1.1.0 for Rust. Because HConsed does not have bounds on its Send trait or Sync trait, memory corruption can occur.	7.5	More Details
CVE-2020-36213	An issue was discovered in the abi_stable crate before 0.9.1 for Rust. A retain call can create an invalid UTF-8 string, violating soundness.	7.5	More Details
CVE-2020-11145	Divide by zero issue can happen while updating delta extension header due to improper validation of master SN and extension header SN in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.5	More Details
CVE-2020-11139	Out of bound memory access while processing frames due to lack of check of invalid frames received in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11119	Buffer over-read can happen when the buffer length received from response handlers is more than the size of the payload in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2020-36212	An issue was discovered in the abi_stable crate before 0.9.1 for Rust. DrainFilter lacks soundness because of a double drop.	7.5	More Details
CVE-2020-8295	A wrong check in Nextcloud Server 19 and prior allowed to perform a denial of service attack when resetting the password for a user.	7.5	More Details
CVE-2021-3115	Go before 1.14.14 and 1.15.x before 1.15.7 on Windows is vulnerable to Command Injection and remote code execution when using the "go get" command to fetch modules that make use of cgo (for example, cgo can execute a gcc program from an untrusted download).	7.5	More Details
CVE-2020-12513	Pepperl+Fuchs Comtrol IO-Link Master in Version 1.5.48 and below is prone to an authenticated blind OS Command Injection.	7.5	More Details
CVE-2020-19360	Local file inclusion in FHEM 6.0 allows in fhem/FileLog_logWrapper file parameter can allow an attacker to include a file, which can lead to sensitive information disclosure.	7.5	More Details
CVE-2020-27858	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CA Arcserve D2D 16.5. Authentication is not required to exploit this vulnerability. The specific flaw exists within the getNews method. Due to the improper restriction of XML External Entity (XXE) references, a specially-crafted document specifying a URI causes the XML parser to access the URI and embed the contents back into the XML document for further processing. An attacker can leverage this vulnerability to disclose information in the context of SYSTEM. Was ZDI-CAN-11103.	7.5	More Details
CVE-2020-27859	This vulnerability allows remote attackers to disclose sensitive information on affected installations of NEC ESMPRO Manager 6.42. Authentication is not required to exploit this vulnerability. The specific flaw exists within the GetEuaLogDownloadAction class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of SYSTEM. Was ZDI-CAN-9607.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21259	HedgeDoc is open source software which lets you create real-time collaborative markdown notes. In HedgeDoc before version 1.7.2, an attacker can inject arbitrary JavaScript into a HedgeDoc note, which is executed when the note is viewed in slide mode. Depending on the configuration of the instance, the attacker may not need authentication to create or edit notes. The problem is patched in HedgeDoc 1.7.2. As a workaround, disallow loading JavaScript from 3rd party sites using the `Content-Security-Policy` header. Note that this will break some embedded content.	7.4	More Details
CVE-2020-12525	M&M Software fdtCONTAINER Component in versions below 3.5.20304.x and between 3.6 and 3.6.20304.x is vulnerable to deserialization of untrusted data in its project storage.	7.3	More Details
CVE-2020-29000	An issue was discovered on Geeni GNC-CW013 doorbell 1.8.1 devices. A vulnerability exists in the RTSP service that allows a remote attacker to take full control of the device with a high-privileged account. By sending a crafted message, an attacker is able to remotely deliver a telnet session. Any attacker that has the ability to control DNS can exploit this vulnerability to remotely login to the device and gain access to the camera system.	7.2	More Details
CVE-2020-28999	An issue was discovered in Apexis Streaming Video Web Application on Geeni GNC-CW013 doorbell 1.8.1 devices. A remote attacker can take full control of the camera with a high-privileged account. The vulnerability exists because a static username and password are compiled into a shared library (libhipcam.so) used to provide the streaming camera service.	7.2	More Details
CVE-2021-2109	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). 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 high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. 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-2020-22643	Feehi CMS 2.1.0 is affected by an arbitrary file upload vulnerability, potentially resulting in remote code execution. After an administrator logs in, open the administrator image upload page to potentially upload malicious files.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29001	An issue was discovered on Geeni GNC-CW028 Camera 2.7.2, Geeni GNC-CW025 Doorbell 2.9.5, Merkury MI-CW024 Doorbell 2.9.6, and Merkury MI-CW017 Camera 2.9.6 devices. A vulnerability exists in the RESTful Services API that allows a remote attacker to take full control of the camera with a high-privileged account. The vulnerability exists because a static username and password are compiled into the ppsapp RESTful application.	7.2	More Details
CVE-2021-3291	Zen Cart 1.5.7b allows admins to execute arbitrary OS commands by inspecting an HTML radio input element (within the modules edit page) and inserting a command.	7.2	More Details
CVE-2021-2054	Vulnerability in the RDBMS Sharding component of Oracle Database Server. Supported versions that are affected are 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Any Procedure, Create Any View, Create Any Trigger privilege with network access via Oracle Net to compromise RDBMS Sharding. Successful attacks of this vulnerability can result in takeover of RDBMS Sharding. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2021-1070	NVIDIA Jetson AGX Xavier Series, Jetson Xavier NX, TX1, TX2, Nano and Nano 2GB, L4T versions prior to 32.5, contains a vulnerability in the apply_binaries.sh script used to install NVIDIA components into the root file system image, in which improper access control is applied, which may lead to an unprivileged user being able to modify system device tree files, leading to denial of service.	7.1	More Details
CVE-2020-28483	This affects all versions of package github.com/gin-gonic/gin. When gin is exposed directly to the internet, a client's IP can be spoofed by setting the X-Forwarded-For header.	7.1	More Details
CVE-2020-36207	An issue was discovered in the aovec crate through 2020-12-10 for Rust. Because Aovec<T> does not have bounds on its Send trait or Sync trait, a data race and memory corruption can occur.	7.0	More Details
CVE-2020-36209	An issue was discovered in the late-static crate before 0.4.0 for Rust. Because Sync is implemented for LateStatic with T: Send, a data race can occur.	7.0	More Details
CVE-2020-11179	Arbitrary read and write to kernel addresses by temporarily overwriting ring buffer pointer and creating a race condition. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36211	An issue was discovered in the gfwx crate before 0.3.0 for Rust. Because ImageChunkMut does not have bounds on its Send trait or Sync trait, a data race and memory corruption can occur.	7.0	More Details
CVE-2020-36206	An issue was discovered in the rusb crate before 0.7.0 for Rust. Because of a lack of Send and Sync bounds, a data race and memory corruption can occur.	7.0	More Details
CVE-2021-1067	NVIDIA SHIELD TV, all versions prior to 8.2.2, contains a vulnerability in the implementation of the RPMB command status, in which an attacker can write to the Write Protect Configuration Block, which may lead to denial of service or escalation of privileges.	6.8	More Details
CVE-2020-28487	This affects the package vis-timeline before 7.4.4. An attacker with the ability to control the items of a Timeline element can inject additional script code into the generated application.	6.8	More Details
CVE-2020-27542	Rostelecom CS-C2SHW 5.0.082.1 is affected by: Bash command injection. The camera reads configuration from QR code (including network settings). The static IP configuration from QR code is copied to the file /config/ip-static and after reboot data from this file is inserted into bash command (without any escaping). So bash injection is possible. Camera doesn't parse QR codes if it's already successfully configured. Camera is always rebooted after successful configuration via QR code.	6.8	More Details
CVE-2021-2046	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, 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 MySQL Server. CVSS 3.1 Base Score 6.8 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H).	6.8	More Details
CVE-2020-11150	Out of bound memory access in camera driver due to improper validation on data coming from UMD which is used for offset manipulation of pointer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11148	Use after free issue in HIDL while using callback to post event in Rx thread when internal mutex is not acquired and meantime close is triggered and callback instance is deleted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	6.7	More Details
CVE-2020-11149	Out of bound access due to usage of an out-of-range pointer offset in the camera driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	6.7	More Details
CVE-2020-11183	A process can potentially cause a buffer overflow in the display service allowing privilege escalation by executing code as that service in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	6.7	More Details
CVE-2020-12514	Pepperl+Fuchs Comtrol IO-Link Master in Version 1.5.48 and below is prone to a NULL Pointer Dereference that leads to a DoS in discoveryd	6.6	More Details
CVE-2021-21238	PySAML2 is a pure python implementation of SAML Version 2 Standard. PySAML2 before 6.5.0 has an improper verification of cryptographic signature vulnerability. All users of pysaml2 that need to validate signed SAML documents are impacted. The vulnerability is a variant of XML Signature wrapping because it did not validate the SAML document against an XML schema. This allowed invalid XML documents to be processed and such a document can trick pysaml2 with a wrapped signature. This is fixed in PySAML2 6.5.0.	6.5	More Details
CVE-2021-1259	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct path traversal attacks and obtain write access to sensitive files on an affected system. The vulnerability is due to insufficient validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to an affected system. A successful exploit could allow the attacker to write arbitrary files on the affected system.	6.5	More Details
CVE-2020-4968	IBM Security Identity Governance and Intelligence 5.2.6 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 192427.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1349	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct Cypher query language injection attacks on an affected system. The vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to the interface of an affected system. A successful exploit could allow the attacker to obtain sensitive information.	6.5	More Details
CVE-2021-1265	A vulnerability in the configuration archive functionality of Cisco DNA Center could allow any privilege-level authenticated, remote attacker to obtain the full unmasked running configuration of managed devices. The vulnerability is due to the configuration archives files being stored in clear text, which can be retrieved by various API calls. An attacker could exploit this vulnerability by authenticating to the device and executing a series of API calls. A successful exploit could allow the attacker to retrieve the full unmasked running configurations of managed devices.	6.5	More Details
CVE-2021-21239	PySAML2 is a pure python implementation of SAML Version 2 Standard. PySAML2 before 6.5.0 has an improper verification of cryptographic signature vulnerability. Users of pysaml2 that use the default CryptoBackendXmlSec1 backend and need to verify signed SAML documents are impacted. PySAML2 does not ensure that a signed SAML document is correctly signed. The default CryptoBackendXmlSec1 backend is using the xmlsec1 binary to verify the signature of signed SAML documents, but by default xmlsec1 accepts any type of key found within the given document. xmlsec1 needs to be configured explicitly to only use only _x509 certificates_ for the verification process of the SAML document signature. This is fixed in PySAML2 6.5.0.	6.5	More Details
CVE-2021-2020	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2128	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	6.5	More Details
CVE-2021-2024	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2021-1253	Multiple vulnerabilities in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow a remote attacker with network-operator privileges to conduct a cross-site scripting (XSS) attack or a reflected file download (RFD) attack against a user of the interface. For more information about these vulnerabilities, see the Details section of this advisory.	6.5	More Details
CVE-2021-1995	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 and 12.1.3.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N).	6.5	More Details
CVE-2020-19363	Vtiger CRM v7.2.0 allows an attacker to display hidden files, list directories by using /libraries and /layout directories.	6.5	More Details
CVE-2021-3114	In Go before 1.14.14 and 1.15.x before 1.15.7, crypto/elliptic/p224.go can generate incorrect outputs, related to an underflow of the lowest limb during the final complete reduction in the P-224 field.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1282	Multiple vulnerabilities in Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) could allow an attacker to conduct path traversal attacks and SQL injection attacks on an affected system. One of the SQL injection vulnerabilities that affects Unified CM IM&P also affects Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) and could allow an attacker to conduct SQL injection attacks on an affected system. For more information about these vulnerabilities, see the Details section of this advisory.	6.5	More Details
CVE-2021-26272	It was possible to execute a ReDoS-type attack inside CKEditor 4 before 4.16 by persuading a victim to paste crafted URL-like text into the editor, and then press Enter or Space (in the Autolink plugin).	6.5	More Details
CVE-2021-2044	Vulnerability in the PeopleSoft Enterprise FIN Payables product of Oracle PeopleSoft (component: Financial Sanctions). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise FIN Payables. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise FIN Payables 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-2021-1355	Multiple vulnerabilities in Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) could allow an attacker to conduct path traversal attacks and SQL injection attacks on an affected system. One of the SQL injection vulnerabilities that affects Unified CM IM&P also affects Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) and could allow an attacker to conduct SQL injection attacks on an affected system. For more information about these vulnerabilities, see the Details section of this advisory.	6.5	More Details
CVE-2021-1357	Multiple vulnerabilities in Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) could allow an attacker to conduct path traversal attacks and SQL injection attacks on an affected system. One of the SQL injection vulnerabilities that affects Unified CM IM&P also affects Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) and could allow an attacker to conduct SQL injection attacks 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-2021-1364	Multiple vulnerabilities in Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) could allow an attacker to conduct path traversal attacks and SQL injection attacks on an affected system. One of the SQL injection vulnerabilities that affects Unified CM IM&P also affects Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) and could allow an attacker to conduct SQL injection attacks on an affected system. For more information about these vulnerabilities, see the Details section of this advisory.	6.5	More Details
CVE-2020-27298	Philips Interventional Workspot (Release 1.3.2, 1.4.0, 1.4.1, 1.4.3, 1.4.5), Coronary Tools/Dynamic Coronary Roadmap/Stentboost Live (Release 1.0), ViewForum (Release 6.3V1L10). The software constructs all or part of an OS command using externally influenced input from an upstream component but does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when sent to a downstream component.	6.5	More Details
CVE-2021-26271	It was possible to execute a ReDoS-type attack inside CKEditor 4 before 4.16 by persuading a victim to paste crafted text into the Styles input of specific dialogs (in the Advanced Tab for Dialogs plugin).	6.5	More Details
CVE-2020-23161	Local file inclusion in Pyrescom Termod4 time management devices before 10.04k allows authenticated remote attackers to traverse directories and read sensitive files via the Maintenance > Logs menu and manipulating the file-path in the URL.	6.5	More Details
CVE-2020-8293	A missing input validation in Nextcloud Server before 20.0.2, 19.0.5, 18.0.11 allows users to store unlimited data in workflow rules causing load and potential DDoS on later interactions and usage with those rules.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21271	Tendermint Core is an open source Byzantine Fault Tolerant (BFT) middleware that takes a state transition machine - written in any programming language - and securely replicates it on many machines. Tendermint Core v0.34.0 introduced a new way of handling evidence of misbehavior. As part of this, we added a new Timestamp field to Evidence structs. This timestamp would be calculated using the same algorithm that is used when a block is created and proposed. (This algorithm relies on the timestamp of the last commit from this specific block.) In Tendermint Core v0.34.0-v0.34.2, the consensus reactor is responsible for forming DuplicateVoteEvidence whenever double signs are observed. However, the current block is still “in flight” when it is being formed by the consensus reactor. It hasn’t been finalized through network consensus yet. This means that different nodes in the network may observe different “last commits” when assigning a timestamp to DuplicateVoteEvidence. In turn, different nodes could form DuplicateVoteEvidence objects at the same height but with different timestamps. One DuplicateVoteEvidence object (with one timestamp) will then eventually get finalized in the block, but this means that any DuplicateVoteEvidence with a different timestamp is considered invalid. Any node that formed invalid DuplicateVoteEvidence will continue to propose invalid evidence; its peers may see this, and choose to disconnect from this node. This bug means that double signs are DoS vectors in Tendermint Core v0.34.0-v0.34.2. Tendermint Core v0.34.3 is a security release which fixes this bug. As of v0.34.3, DuplicateVoteEvidence is no longer formed by the consensus reactor; rather, the consensus reactor passes the Votes themselves into the EvidencePool, which is now responsible for forming DuplicateVoteEvidence. The EvidencePool has timestamp info that should be consistent across the network, which means that DuplicateVoteEvidence formed in this reactor should have consistent timestamps. This release changes the API between the consensus and evidence reactors.	6.5	More Details
CVE-2021-1286	Multiple vulnerabilities in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow a remote attacker with network-operator privileges to conduct a cross-site scripting (XSS) attack or a reflected file download (RFD) attack against a user of the interface. For more information about these vulnerabilities, see the Details section of this advisory.	6.5	More Details
CVE-2020-36200	TinyCheck before commits 9fd360d and ea53de8 allowed an authenticated attacker to send an HTTP GET request to the crafted URLs.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1249	Multiple vulnerabilities in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow a remote attacker with network-operator privileges to conduct a cross-site scripting (XSS) attack or a reflected file download (RFD) attack against a user of the interface. For more information about these vulnerabilities, see the Details section of this advisory.	6.5	More Details
CVE-2021-1250	Multiple vulnerabilities in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow a remote attacker with network-operator privileges to conduct a cross-site scripting (XSS) attack or a reflected file download (RFD) attack against a user of the interface. For more information about these vulnerabilities, see the Details section of this advisory.	6.5	More Details
CVE-2020-11152	Race condition in HAL layer while processing callback objects received from HIDL due to lack of synchronization between accessing objects in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	6.4	More Details
CVE-2020-11151	Race condition occurs while calling user space ioctl from two different threads can results to use after free issue in video in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	6.4	More Details
CVE-2020-8554	Kubernetes API server in all versions allow an attacker who is able to create a ClusterIP service and set the spec.externalIPs field, to intercept traffic to that IP address. Additionally, an attacker who is able to patch the status (which is considered a privileged operation and should not typically be granted to users) of a LoadBalancer service can set the status.loadBalancer.ingress.ip to similar effect.	6.3	More Details
CVE-2021-23326	This affects the package @graphql-tools/git-loader before 6.2.6. The use of exec and execSync in packages/loaders/git/src/load-git.ts allows arbitrary command injection.	6.3	More Details
CVE-2021-1270	Multiple vulnerabilities in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to view, modify, and delete data without proper authorization. For more information about these vulnerabilities, see the Details section of this advisory.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1269	Multiple vulnerabilities in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to view, modify, and delete data without proper authorization. For more information about these vulnerabilities, see the Details section of this advisory.	6.3	More Details
CVE-2021-2057	Vulnerability in the Oracle Retail Customer Management and Segmentation Foundation product of Oracle Retail Applications (component: Internal Operations). The supported version that is affected is 19.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Retail Customer Management and Segmentation Foundation. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Retail Customer Management and Segmentation Foundation accessible data as well as unauthorized read access to a subset of Oracle Retail Customer Management and Segmentation Foundation accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Retail Customer Management and Segmentation Foundation. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).	6.3	More Details
CVE-2020-28452	This affects the package com.softwaremill.akka-http-session:core_2.12 from 0 and before 0.6.1; all versions of package com.softwaremill.akka-http-session:core_2.11; the package com.softwaremill.akka-http-session:core_2.13 from 0 and before 0.6.1. CSRF protection can be bypassed by forging a request that contains the same value for both the X-XSRF-TOKEN header and the XSRF-TOKEN cookie value, as the check in randomTokenCsrfProtection only checks that the two values are equal and non-empty.	6.3	More Details
CVE-2021-21270	OctopusDSC is a PowerShell module with DSC resources that can be used to install and configure an Octopus Deploy Server and Tentacle agent. In OctopusDSC version 4.0.977 and earlier a customer API key used to connect to Octopus Server is exposed via logging in plaintext. This vulnerability is patched in version 4.0.1002.	6.2	More Details
CVE-2021-1069	NVIDIA SHIELD TV, all versions prior to 8.2.2, contains a vulnerability in the NVHost function, which may lead to abnormal reboot due to a null pointer reference, causing data loss.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13133	Tufin SecureChange prior to R19.3 HF3 and R20-1 HF1 are vulnerable to stored XSS. The successful exploitation requires admin privileges (for storing the XSS payload itself), and can exploit (be triggered by) unauthenticated users. All TOS versions with SecureChange deployments prior to R19.3 HF3 and R20-1 HF1 are affected. Vulnerabilities were fixed in R19.3 HF3 and R20-1 HF1	6.1	More Details
CVE-2020-24085	A cross-site scripting (XSS) vulnerability exists in MISP v2.4.128 in app/Controller/UserSettingsController.php at SetHomePage() function. Due to a lack of controller validation in "path" parameter, an attacker can execute malicious JavaScript code.	6.1	More Details
CVE-2020-23774	A reflected XSS vulnerability exists in tohtml/convert.php of Winmail 6.5, which can cause JavaScript code to be executed.	6.1	More Details
CVE-2020-25385	Nagios Log Server 2.1.7 contains a cross-site scripting (XSS) vulnerability in /nagioslogserver/configure/create_snapshot through the snapshot_name parameter, which may impact users who open a maliciously crafted link or third-party web page.	6.1	More Details
CVE-2020-19362	Reflected XSS in Vtiger CRM v7.2.0 in vtigercrm/index.php? through the view parameter can result in an attacker performing malicious actions to users who open a maliciously crafted link or third-party web page.	6.1	More Details
CVE-2021-2040	Vulnerability in the Oracle Argus Safety product of Oracle Health Sciences Applications (component: Case Form, Local Affiliate Form). The supported version that is affected is 8.2.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Argus Safety. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Argus Safety, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Argus Safety accessible data as well as unauthorized read access to a subset of Oracle Argus Safety 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-2021-22873	Revive Adserver before 5.1.0 is vulnerable to open redirects via the `dest`, `oadest`, and/or `ct0` parameters of the lg.php and ck.php delivery scripts. Such open redirects had previously been available by design to allow third party ad servers to track such metrics when delivering ads. However, third party click tracking via redirects is not a viable option anymore, leading to such open redirect functionality being removed and reclassified as a vulnerability.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27735	An XSS issue was discovered in Wing FTP 6.4.4. An arbitrary IFRAME element can be included in the help pages via a crafted link, leading to the execution of (sandboxed) arbitrary HTML and JavaScript in the user's browser.	6.1	More Details
CVE-2020-35753	The job posting recommendation form in Persis Human Resource Management Portal (Versions 17.2.00 through 17.2.35 and 19.0.00 through 19.0.20), when the "Recommend job posting" function is enabled, allows XSS via the SENDER parameter.	6.1	More Details
CVE-2021-2043	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2020-19361	Reflected XSS in Medintux v2.16.000 CCAM.php by manipulating the mot1 parameter can result in an attacker performing malicious actions to users who open a maliciously crafted link or third-party web page.	6.1	More Details
CVE-2020-21146	Feehi CMS 2.0.8 is affected by a cross-site scripting (XSS) vulnerability. When the user name is inserted as JavaScript code, browsing the post will trigger the XSS.	6.1	More Details
CVE-2020-23447	newbee-mall 1.0 is affected by cross-site scripting in shop-cart/settle. Users only need to write xss payload in their address information when buying goods, which is triggered when viewing the "View Recipient Information" of this order in "Order Management Office".	6.1	More Details
CVE-2020-36202	An issue was discovered in the async-h1 crate before 2.3.0 for Rust. Request smuggling can occur when used behind a reverse proxy.	6.1	More Details
CVE-2021-3186	A Stored Cross-site scripting (XSS) vulnerability in /main.html Wifi Settings in Tenda AC5 AC1200 version V15.03.06.47_multi allows remote attackers to inject arbitrary web script or HTML via the Wifi Name parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22872	Revive Adserver before 5.1.0 is vulnerable to a reflected cross-site scripting (XSS) vulnerability via the publicly accessible afr.php delivery script. While this issue was previously addressed in modern browsers as CVE-2020-8115, some older browsers (e.g., IE10) that do not automatically URL encode parameters were still vulnerable.	6.1	More Details
CVE-2021-2120	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. 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 access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details
CVE-2021-2086	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. 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-2021-2124	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. 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 Number	Description	Base Score	Reference
CVE-2021-2119	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. 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 access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details
CVE-2021-2111	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. 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-2021-2131	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. 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 creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N).	6.0	More Details
CVE-2021-2112	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. 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 Number	Description	Base Score	Reference
CVE-2021-2126	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. 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 creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N).	6.0	More Details
CVE-2021-2121	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. 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-2020-36219	An issue was discovered in the atomic-option crate through 2020-10-31 for Rust. Because AtomicOption<T> implements Sync unconditionally, a data race can occur.	5.9	More Details
CVE-2021-2011	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client. 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-2020-36218	An issue was discovered in the buttplug crate before 1.0.4 for Rust. ButtplugFutureStateShared does not properly consider (!Send!Sync) objects, leading to a data race.	5.9	More Details
CVE-2020-36216	An issue was discovered in Input<R> in the eventio crate before 0.5.1 for Rust. Because a non-Send type can be sent to a different thread, a data race and memory corruption can occur.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36214	An issue was discovered in the multiqueue2 crate before 0.1.7 for Rust. Because a non-Send type can be sent to a different thread, a data race can occur.	5.9	More Details
CVE-2020-20949	Bleichenbacher's attack on PKCS #1 v1.5 padding for RSA in STM32 cryptographic firmware library software expansion for STM32Cube (UM1924). The vulnerability can allow one to use Bleichenbacher's oracle attack to decrypt an encrypted ciphertext by making successive queries to the server using the vulnerable library, resulting in remote information disclosure.	5.9	More Details
CVE-2020-36220	An issue was discovered in the va-ts crate before 0.0.4 for Rust. Because Demuxer<T> omits a required T: Send bound, a data race and memory corruption can occur.	5.9	More Details
CVE-2020-25687	A flaw was found in dnsmasq before version 2.83. A heap-based buffer overflow was discovered in dnsmasq when DNSSEC is enabled and before it validates the received DNS entries. This flaw allows a remote attacker, who can create valid DNS replies, to cause an overflow in a heap-allocated memory. This flaw is caused by the lack of length checks in rfc1035.c:extract_name(), which could be abused to make the code execute memcpy() with a negative size in sort_rrset() and cause a crash in dnsmasq, resulting in a denial of service. The highest threat from this vulnerability is to system availability.	5.9	More Details
CVE-2020-4969	IBM Security Identity Governance and Intelligence 5.2.6 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques.	5.9	More Details
CVE-2021-3130	Within the Open-AudIT up to version 3.5.3 application, the web interface hides SSH secrets, Windows passwords, and SNMP strings from users using HTML 'password field' obfuscation. By using Developer tools or similar, it is possible to change the obfuscation so that the credentials are visible.	5.9	More Details
CVE-2020-36217	An issue was discovered in the may_queue crate through 2020-11-10 for Rust. Because Queue does not have bounds on its Send trait or Sync trait, memory corruption can occur.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25683	A flaw was found in dnsmasq before version 2.83. A heap-based buffer overflow was discovered in dnsmasq when DNSSEC is enabled and before it validates the received DNS entries. A remote attacker, who can create valid DNS replies, could use this flaw to cause an overflow in a heap-allocated memory. This flaw is caused by the lack of length checks in rfc1035.c:extract_name(), which could be abused to make the code execute memcpy() with a negative size in get_rdata() and cause a crash in dnsmasq, resulting in a denial of service. The highest threat from this vulnerability is to system availability.	5.9	More Details
CVE-2020-17522	When ORT (now via atstccfg) generates ip_allow.config files in Apache Traffic Control 3.0.0 to 3.1.0 and 4.0.0 to 4.1.0, those files include permissions that allow bad actors to push arbitrary content into and remove arbitrary content from CDN cache servers. Additionally, these permissions are potentially extended to IP addresses outside the desired range, resulting in them being granted to clients possibly outside the CDN arcitechture.	5.8	More Details
CVE-2021-21253	OnlineVotingSystem is an open source project hosted on GitHub. OnlineVotingSystem before version 1.1.2 hashes user passwords without a salt, which is vulnerable to dictionary attacks. Therefore there is a threat of security breach in the voting system. Without a salt, it is much easier for attackers to pre-compute the hash value using dictionary attack techniques such as rainbow tables to crack passwords. This problem is fixed and published in version 1.1.2. A long randomly generated salt is added to the password hash function to better protect passwords stored in the voting system.	5.8	More Details
CVE-2020-8568	Kubernetes Secrets Store CSI Driver versions v0.0.15 and v0.0.16 allow an attacker who can modify a SecretProviderClassPodStatus/Status resource the ability to write content to the host filesystem and sync file contents to Kubernetes Secrets. This includes paths under var/lib/kubelet/pods that contain other Kubernetes Secrets.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26278	Weave Net is open source software which creates a virtual network that connects Docker containers across multiple hosts and enables their automatic discovery. Weave Net before version 2.8.0 has a vulnerability in which can allow an attacker to take over any host in the cluster. Weave Net is supplied with a manifest that runs pods on every node in a Kubernetes cluster, which are responsible for managing network connections for all other pods in the cluster. This requires a lot of power over the host, and the manifest sets `privileged: true`, which gives it that power. It also set `hostPID: true`, which gave it the ability to access all other processes on the host, and write anywhere in the root filesystem of the host. This setting was not necessary, and is being removed. You are only vulnerable if you have an additional vulnerability (e.g. a bug in Kubernetes) or misconfiguration that allows an attacker to run code inside the Weave Net pod, No such bug is known at the time of release, and there are no known instances of this being exploited. Weave Net 2.8.0 removes the hostPID setting and moves CNI plugin install to an init container. Users who do not update to 2.8.0 can edit the hostPID line in their existing DaemonSet manifest to say false instead of true, arrange some other way to install CNI plugins (e.g. Ansible) and remove those mounts from the DaemonSet manifest.	5.8	More Details
CVE-2021-1353	A vulnerability in the IPv4 protocol handling of Cisco StarOS could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a memory leak that occurs during packet processing. An attacker could exploit this vulnerability by sending a series of crafted IPv4 packets through an affected device. A successful exploit could allow the attacker to exhaust the available memory and cause an unexpected restart of the npusim process, leading to a DoS condition on the affected device.	5.8	More Details
CVE-2021-2052	Vulnerability in the JD Edwards EnterpriseOne Orchestrator product of Oracle JD Edwards (component: E1 IOT Orchestrator Security). The supported version that is affected is Prior to 9.2.5.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Orchestrator. While the vulnerability is in JD Edwards EnterpriseOne Orchestrator, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of JD Edwards EnterpriseOne Orchestrator accessible data. CVSS 3.1 Base Score 5.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N).	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1071	NVIDIA Tegra kernel in Jetson AGX Xavier Series, Jetson Xavier NX, TX1, TX2, Nano and Nano 2GB, all L4T versions prior to r32.5, contains a vulnerability in the INA3221 driver in which improper access control may lead to unauthorized users gaining access to system power usage data, which may lead to information disclosure.	5.6	More Details
CVE-2020-36205	An issue was discovered in the xcb crate through 2020-12-10 for Rust. base::Error does not have soundness. Because of the public ptr field, a use-after-free or double-free can occur.	5.5	More Details
CVE-2021-1283	A vulnerability in the logging subsystem of Cisco Data Center Network Manager (DCNM) could allow an authenticated, local attacker to view sensitive information in a system log file that should be restricted. The vulnerability exists because sensitive information is not properly masked before it is written to system log files. An attacker could exploit this vulnerability by authenticating to an affected device and inspecting a specific system log file. A successful exploit could allow the attacker to view sensitive information in the system log file. To exploit this vulnerability, the attacker would need to have valid user credentials.	5.5	More Details
CVE-2021-1235	A vulnerability in the CLI of Cisco SD-WAN vManage Software could allow an authenticated, local attacker to read sensitive database files on an affected system. The vulnerability is due to insufficient user authorization. An attacker could exploit this vulnerability by accessing the vshell of an affected system. A successful exploit could allow the attacker to read database files from the filesystem of the underlying operating system.	5.5	More Details
CVE-2020-27098	In checkGrantUriPermission of UriGrantsManagerService.java, there is a possible way to access contacts due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-138791358	5.5	More Details
CVE-2020-27097	In checkGrantUriPermission of UriGrantsManagerService.java, there is a possible permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-140729426	5.5	More Details
CVE-2020-4887	IBM AIX 7.1, 7.2 and AIX VIOS 3.1 could allow a local user to exploit a vulnerability in the gencore user command to create arbitrary files in any directory. IBM X-Force ID: 190911.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3308	An issue was discovered in Xen 4.12.3 through 4.12.4 and 4.13.1 through 4.14.x. An x86 HVM guest with PCI pass through devices can force the allocation of all IDT vectors on the system by rebooting itself with MSI or MSI-X capabilities enabled and entries setup. Such reboots will leak any vectors used by the MSI(-X) entries that the guest might had enabled, and hence will lead to vector exhaustion on the system, not allowing further PCI pass through devices to work properly. HVM guests with PCI pass through devices can mount a Denial of Service (DoS) attack affecting the pass through of PCI devices to other guests or the hardware domain. In the latter case, this would affect the entire host.	5.5	More Details
CVE-2020-26941	A local (authenticated) low-privileged user can exploit a behavior in an ESET installer to achieve arbitrary file overwrite (deletion) of any file via a symlink, due to insecure permissions. The possibility of exploiting this vulnerability is limited and can only take place during the installation phase of ESET products. Furthermore, exploitation can only succeed when Self-Defense is disabled. Affected products are: ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security, ESET Smart Security Premium versions 13.2 and lower; ESET Endpoint Antivirus, ESET Endpoint Security, ESET NOD32 Antivirus Business Edition, ESET Smart Security Business Edition versions 7.3 and lower; ESET File Security for Microsoft Windows Server, ESET Mail Security for Microsoft Exchange Server, ESET Mail Security for IBM Domino, ESET Security for Kerio, ESET Security for Microsoft SharePoint Server versions 7.2 and lower.	5.5	More Details
CVE-2020-35843	FastStone Image Viewer 7.5 has an out-of-bounds write (via a crafted image file) at FSViewer.exe+0x956e.	5.5	More Details
CVE-2020-3687	Local privilege escalation in admin services in Windows environment can occur due to an arbitrary read issue.	5.5	More Details
CVE-2020-27851	Multiple stored HTML injection vulnerabilities in the "poll" and "quiz" features in an additional paid add-on of Rocketgenius Gravity Forms before 2.4.21 allows remote attackers to inject arbitrary HTML code via poll or quiz answers. This code is interpreted by users in a privileged role (Administrator, Editor, etc.).	5.4	More Details
CVE-2020-8288	The `specializedRendering` function in Rocket.Chat server before 3.9.2 allows a cross-site scripting (XSS) vulnerability by way of the `value` parameter.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2117	Vulnerability in the Oracle Application Express Survey Builder component of Oracle Database Server. The supported version that is affected is Prior to 20.2. Easily exploitable vulnerability allows low privileged attacker having Valid User Account privilege with network access via HTTP to compromise Oracle Application Express Survey Builder. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express Survey Builder, 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 Survey Builder accessible data as well as unauthorized read access to a subset of Oracle Application Express Survey Builder 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-2020-27852	A stored Cross-Site Scripting (XSS) vulnerability in the survey feature in Rocketgenius Gravity Forms before 2.4.21 allows remote attackers to inject arbitrary web script or HTML via a textarea field. This code is interpreted by users in a privileged role (Administrator, Editor, etc.).	5.4	More Details
CVE-2021-2003	Vulnerability in the Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web Dashboards). 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 Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Business Intelligence Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2021-3137	XWiki 12.10.2 allows XSS via an SVG document to the upload feature of the comment section.	5.4	More Details
CVE-2020-8292	Rocket.Chat server before 3.9.0 is vulnerable to a self cross-site scripting (XSS) vulnerability via the drag & drop functionality in message boxes.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2116	Vulnerability in the Oracle Application Express Opportunity Tracker component of Oracle Database Server. The supported version that is affected is Prior to 20.2. Easily exploitable vulnerability allows low privileged attacker having Valid User Account privilege with network access via HTTP to compromise Oracle Application Express Opportunity Tracker. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express Opportunity Tracker, 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 Opportunity Tracker accessible data as well as unauthorized read access to a subset of Oracle Application Express Opportunity Tracker 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-2021-1218	A vulnerability in the web management interface of Cisco Smart Software Manager satellite could allow an authenticated, remote attacker to redirect a user to an undesired web page. The vulnerability is due to improper input validation of the URL parameters in an HTTP request that is sent to an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request that could cause the web application to redirect the request to a specified malicious URL. A successful exploit could allow the attacker to redirect a user to a malicious website.	5.4	More Details
CVE-2020-23014	APfell 1.4 is vulnerable to authenticated reflected cross-site scripting (XSS) in /apiui/command_ through the payloadtypes_callback function, which allows an attacker to steal remote admin/user session and/or adding new users to the administration panel.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21283	Flarum is an open source discussion platform for websites. The "Flarum Sticky" extension versions 0.1.0-beta.14 and 0.1.0-beta.15 has a cross-site scripting vulnerability. A change in release beta 14 of the Sticky extension caused the plain text content of the first post of a pinned discussion to be injected as HTML on the discussion list. The issue was discovered following an internal audit. Any HTML would be injected through the m.trust() helper. This resulted in an HTML injection where <script> tags would not be executed. However it was possible to run javascript from other HTML attributes, enabling a cross-site scripting (XSS) attack to be performed. Since the exploit only happens with the first post of a pinned discussion, an attacker would need the ability to pin their own discussion, or be able to edit a discussion that was previously pinned. On forums where all pinned posts are authored by your staff, you can be relatively certain the vulnerability has not been exploited. Forums where some user-created discussions were pinned can look at the first post edit date to find whether the vulnerability might have been exploited. Because Flarum doesn't store the post content history, you cannot be certain if a malicious edit was reverted. The fix will be available in version v0.1.0-beta.16 with Flarum beta 16. The fix has already been back-ported to Flarum beta 15 as version v0.1.0-beta.15.1 of the Sticky extension. Forum administrators can disable the Sticky extension until they are able to apply the update. The vulnerability cannot be exploited while the extension is disabled.	5.4	More Details
CVE-2019-25015	LuCI in OpenWrt 18.06.0 through 18.06.4 allows stored XSS via a crafted SSID.	5.4	More Details
CVE-2021-21615	Jenkins 2.275 and LTS 2.263.2 allows reading arbitrary files using the file browser for workspaces and archived artifacts due to a time-of-check to time-of-use (TOCTOU) race condition.	5.3	More Details
CVE-2021-21275	The MediaWiki "Report" extension has a Cross-Site Request Forgery (CSRF) vulnerability. Before fixed version, there was no protection against CSRF checks on Special:Report, so requests to report a revision could be forged. The problem has been fixed in commit f828dc6 by making use of MediaWiki edit tokens.	5.3	More Details
CVE-2021-3285	jxbrowser in TI Code Composer Studio IDE 8.x through 10.x before 10.1.1 does not verify X.509 certificates for HTTPS.	5.3	More Details
CVE-2021-25901	An issue was discovered in the lazy-init crate through 2021-01-17 for Rust. Lazy lacks a Send bound, leading to a data race.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2006	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 8.0.19 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).	5.3	More Details
CVE-2021-2059	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Web interface). 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 iStore. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle iStore 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-2021-1312	A vulnerability in the system resource management of Cisco Elastic Services Controller (ESC) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) to the health monitor API on an affected device. The vulnerability is due to inadequate provisioning of kernel parameters for the maximum number of TCP connections and SYN backlog. An attacker could exploit this vulnerability by sending a flood of crafted TCP packets to an affected device. A successful exploit could allow the attacker to block TCP listening ports that are used by the health monitor API. This vulnerability only affects customers who use the health monitor API.	5.3	More Details
CVE-2021-1129	A vulnerability in the authentication for the general purpose APIs implementation of Cisco Email Security Appliance (ESA), Cisco Content Security Management Appliance (SMA), and Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to access general system information and certain configuration information from an affected device. The vulnerability exists because a secure authentication token is not required when authenticating to the general purpose API. An attacker could exploit this vulnerability by sending a crafted request for information to the general purpose API on an affected device. A successful exploit could allow the attacker to obtain system and configuration information from the affected device, resulting in an unauthorized information disclosure.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3152	Home Assistant before 2021.1.3 does not have a protection layer that can help to prevent directory-traversal attacks against custom integrations. NOTE: the vendor's perspective is that the vulnerability itself is in custom integrations written by third parties, not in Home Assistant; however, Home Assistant does have a security update that is worthwhile in addressing this situation	5.3	More Details
CVE-2021-1350	A vulnerability in the web UI of Cisco Umbrella could allow an unauthenticated, remote attacker to negatively affect the performance of this service. The vulnerability exists due to insufficient rate limiting controls in the web UI. An attacker could exploit this vulnerability by sending crafted HTTPS packets at a high and sustained rate. A successful exploit could allow the attacker to negatively affect the performance of the web UI. Cisco has addressed this vulnerability.	5.3	More Details
CVE-2021-2048	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.22 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-2021-2110	Vulnerability in the Oracle Argus Safety product of Oracle Health Sciences Applications (component: Letters). The supported version that is affected is 8.2.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Argus Safety. While the vulnerability is in Oracle Argus Safety, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Argus Safety accessible data. CVSS 3.1 Base Score 5.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1999	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: RAS subsystems). The supported version that is affected is 8.8. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle ZFS Storage Appliance Kit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle ZFS Storage Appliance Kit accessible data. CVSS 3.1 Base Score 5.0 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:C/C:N/I:H/A:N).	5.0	More Details
CVE-2021-2016	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 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-2021-2009	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.19 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-2021-2028	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). 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 Number	Description	Base Score	Reference
CVE-2021-2070	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 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-2021-2030	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-2021-2076	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 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-2021-2065	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 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-2021-2060	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.50 and prior, 5.7.32 and prior and 8.0.22 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-2021-2058	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Locking). Supported versions that are affected are 8.0.22 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-2021-2001	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.50 and prior, 5.7.30 and prior and 8.0.17 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-2021-2002	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.22 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-2021-2014	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PAM Auth Plugin). Supported versions that are affected are 5.7.32 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-2021-2031	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 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-2021-2055	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-2020-8567	Kubernetes Secrets Store CSI Driver Vault Plugin prior to v0.0.6, Azure Plugin prior to v0.0.10, and GCP Plugin prior to v0.2.0 allow an attacker who can create specially-crafted SecretProviderClass objects to write to arbitrary file paths on the host filesystem, including /var/lib/kubelet/pods.	4.9	More Details
CVE-2021-2081	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 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-2021-2012	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 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-2021-2036	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 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-2021-2122	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.22 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-2021-2072	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 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-2020-35513	A flaw incorrect umask during file or directory modification in the Linux kernel NFS (network file system) functionality was found in the way user create and delete object using NFSv4.2 or newer if both simultaneously accessing the NFS by the other process that is not using new NFSv4.2. A user with access to the NFS could use this flaw to starve the resources causing denial of service.	4.9	More Details
CVE-2021-2021	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 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-2021-1993	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Java VM. 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 Java VM accessible data. CVSS 3.1 Base Score 4.8 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:N).	4.8	More Details
CVE-2020-21147	RockOA V1.9.8 is affected by a cross-site scripting (XSS) vulnerability which allows remote attackers to send malicious code to the administrator and execute JavaScript code, because webmain/flow/input/mode_emailmAction.php does not perform strict filtering.	4.8	More Details
CVE-2020-27850	A stored Cross-Site Scripting (XSS) vulnerability in forms import feature in Rocketgenius Gravity Forms before 2.4.21 allows remote attackers to inject arbitrary web script or HTML via the import of a GF form. This code is interpreted by users in a privileged role (Administrator, Editor, etc.).	4.8	More Details
CVE-2020-35309	Bakeshop Online Ordering System in PHP/MySQLi 1.0 is affected by cross-site scripting (XSS) which allows remote attackers to inject an arbitrary web script or HTML in admin dashboard - "Categories".	4.8	More Details
CVE-2020-35271	Employee Performance Evaluation System in PHP/MySQLi with Source Code 1.0 is affected by cross-site scripting (XSS) in the Employees, First Name and Last Name fields.	4.8	More Details
CVE-2020-29241	Online News Portal using PHP/MySQLi 1.0 is affected by cross-site scripting (XSS) which allows remote attackers to inject an arbitrary web script or HTML via the "Title" parameter.	4.8	More Details
CVE-2020-35272	Employee Performance Evaluation System in PHP/MySQLi with Source Code 1.0 is affected by cross-site scripting (XSS) in the Admin Portal in the Task and Description fields.	4.8	More Details
CVE-2020-36011	A cross-site scripting (XSS) issue in Add Patient Form in QDOCS Smart Hospital Management System 3.1 allows a remote attacker to inject arbitrary code via the Name, Guardian Name, Email, Address, Remarks, or Any Known Allergies field.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22871	Revive Adserver before 5.1.0 permits any user with a manager account to store possibly malicious content in the URL website property, which is then displayed unsanitized in the affiliate-preview.php tag generation screen, leading to a persistent cross-site scripting (XSS) vulnerability.	4.8	More Details
CVE-2020-35854	Textpattern 4.8.4 is affected by cross-site scripting (XSS) in the Body parameter.	4.8	More Details
CVE-2020-35853	4images Image Gallery Management System 1.7.11 is affected by cross-site scripting (XSS) in the Image URL. This vulnerability can result in an attacker to inject the XSS payload into the IMAGE URL. Each time a user visits that URL, the XSS triggers and the attacker can be able to steal the cookie according to the crafted payload.	4.8	More Details
CVE-2020-13134	Tufin SecureChange prior to R19.3 HF3 and R20-1 HF1 are vulnerable to stored XSS. The successful exploitation requires admin privileges (for storing the XSS payload itself), and can exploit (be triggered by) admin users. All TOS versions with SecureChange deployments prior to R19.3 HF3 and R20-1 HF1 are affected. Vulnerabilities were fixed in R19.3 HF3 and R20-1 HF1.	4.8	More Details
CVE-2021-1271	A vulnerability in the web-based management interface of Cisco AsyncOS for Cisco Web Security Appliance (WSA) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by inserting malicious data into a specific data field in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface.	4.8	More Details
CVE-2020-36204	An issue was discovered in the im crate through 2020-11-09 for Rust. Because TreeFocus does not have bounds on its Send trait or Sync trait, a data race can occur.	4.7	More Details
CVE-2020-36203	An issue was discovered in the reffers crate through 2020-12-01 for Rust. ARefss can contain a !Send,!Sync object, leading to a data race and memory corruption.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2023	Vulnerability in the Oracle Installed Base product of Oracle E-Business Suite (component: APIs). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Installed Base. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Installed Base, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Installed Base accessible data. CVSS 3.1 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	4.7	More Details
CVE-2021-2005	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: BI Platform Security). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 4.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N).	4.7	More Details
CVE-2021-1255	Multiple vulnerabilities in the REST API endpoint of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to view, modify, and delete data without proper authorization. For more information about these vulnerabilities, see the Details section of this advisory.	4.6	More Details
CVE-2021-1133	Multiple vulnerabilities in the REST API endpoint of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to view, modify, and delete data without proper authorization. For more information about these vulnerabilities, see the Details section of this advisory.	4.6	More Details
CVE-2021-1135	Multiple vulnerabilities in the REST API endpoint of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to view, modify, and delete data without proper authorization. For more information about these vulnerabilities, see the Details section of this advisory.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2125	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. 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 update, insert or delete access to some of Oracle VM VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N).	4.6	More Details
CVE-2021-22849	Hyweb HyCMS-J1 backend editing function does not filter special characters. Users after log-in can inject JavaScript syntax to perform a stored XSS (Stored Cross-site scripting) attack.	4.6	More Details
CVE-2021-23272	The Application Development Clients component of TIBCO Software Inc.'s TIBCO BPM Enterprise and TIBCO BPM Enterprise Distribution for TIBCO Silver Fabric contains a vulnerability that theoretically allows a low privileged attacker with network access to execute a Cross Site Scripting (XSS) attack on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO BPM Enterprise: versions 4.3.0 and below and TIBCO BPM Enterprise Distribution for TIBCO Silver Fabric: versions 4.3.0 and below.	4.6	More Details
CVE-2021-2073	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details
CVE-2021-2022	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.6.50 and prior, 5.7.32 and prior and 8.0.22 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 Number	Description	Base Score	Reference
CVE-2021-1233	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information on an affected device. The vulnerability is due to insufficient input validation of requests that are sent to the iperf tool. An attacker could exploit this vulnerability by sending a crafted request to the iperf tool, which is included in Cisco SD-WAN Software. A successful exploit could allow the attacker to obtain any file from the filesystem of an affected device.	4.4	More Details
CVE-2021-2130	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details
CVE-2021-2127	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details
CVE-2021-2038	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.22 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 Number	Description	Base Score	Reference
CVE-2021-2088	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.22 and prior. Easily exploitable 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 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:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details
CVE-2021-2087	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.22 and prior. Easily exploitable 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 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:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details
CVE-2020-6780	Use of Password Hash With Insufficient Computational Effort in the database of Bosch FSM-2500 server and Bosch FSM-5000 server up to and including version 5.2 allows a remote attacker with admin privileges to dump the credentials of other users and possibly recover their plain-text passwords by brute-forcing the MD5 hash.	4.4	More Details
CVE-2021-2056	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.22 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-2021-2061	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.22 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 Number	Description	Base Score	Reference
CVE-2021-2032	Vulnerability in the MySQL Server product of Oracle MySQL (component: Information Schema). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server 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-2021-2004	Vulnerability in the Siebel Core - Server BizLogic Script product of Oracle Siebel CRM (component: Integration - Scripting). Supported versions that are affected are 20.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel Core - Server BizLogic Script. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Siebel Core - Server BizLogic Script 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-2021-2017	Vulnerability in the Oracle User Management product of Oracle E-Business Suite (component: Proxy User Delegation). 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 User Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle User 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-2021-2113	Vulnerability in the Oracle Financial Services Revenue Management and Billing product of Oracle Financial Services Applications (component: On Demand Billing). Supported versions that are affected are 2.9.0.0 and 2.9.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Revenue Management and Billing. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Revenue Management and Billing accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8569	Kubernetes CSI snapshot-controller prior to v2.1.3 and v3.0.2 could panic when processing a VolumeSnapshot custom resource when: - The VolumeSnapshot referenced a non-existing PersistentVolumeClaim and the VolumeSnapshot did not reference any VolumeSnapshotClass. - The snapshot-controller crashes, is automatically restarted by Kubernetes, and processes the same VolumeSnapshot custom resource after the restart, entering an endless crashloop. Only the volume snapshot feature is affected by this vulnerability. When exploited, users can't take snapshots of their volumes or delete the snapshots. All other Kubernetes functionality is not affected.	4.3	More Details
CVE-2020-4966	IBM Security Identity Governance and Intelligence 5.2.6 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: 192423.	4.3	More Details
CVE-2021-2033	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core Components). 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. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic Server. 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-2021-2010	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.50 and prior, 5.7.32 and prior and 8.0.22 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Client accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Client. CVSS 3.1 Base Score 4.2 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:L).	4.2	More Details
CVE-2020-29443	ide_atapi_cmd_reply_end in hw/ide/atapi.c in QEMU 5.1.0 allows out-of-bounds read access because a buffer index is not validated.	3.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1998	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 3.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L).	3.8	More Details
CVE-2020-25684	A flaw was found in dnsmasq before version 2.83. When getting a reply from a forwarded query, dnsmasq checks in the forward.c:reply_query() if the reply destination address/port is used by the pending forwarded queries. However, it does not use the address/port to retrieve the exact forwarded query, substantially reducing the number of attempts an attacker on the network would have to perform to forge a reply and get it accepted by dnsmasq. This issue contrasts with RFC5452, which specifies a query's attributes that all must be used to match a reply. This flaw allows an attacker to perform a DNS Cache Poisoning attack. If chained with CVE-2020-25685 or CVE-2020-25686, the attack complexity of a successful attack is reduced. The highest threat from this vulnerability is to data integrity.	3.7	More Details
CVE-2020-25685	A flaw was found in dnsmasq before version 2.83. When getting a reply from a forwarded query, dnsmasq checks in forward.c:reply_query(), which is the forwarded query that matches the reply, by only using a weak hash of the query name. Due to the weak hash (CRC32 when dnsmasq is compiled without DNSSEC, SHA-1 when it is) this flaw allows an off-path attacker to find several different domains all having the same hash, substantially reducing the number of attempts they would have to perform to forge a reply and get it accepted by dnsmasq. This is in contrast with RFC5452, which specifies that the query name is one of the attributes of a query that must be used to match a reply. This flaw could be abused to perform a DNS Cache Poisoning attack. If chained with CVE-2020-25684 the attack complexity of a successful attack is reduced. The highest threat from this vulnerability is to data integrity.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2007	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Client accessible data. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	3.7	More Details
CVE-2020-25686	A flaw was found in dnsmasq before version 2.83. When receiving a query, dnsmasq does not check for an existing pending request for the same name and forwards a new request. By default, a maximum of 150 pending queries can be sent to upstream servers, so there can be at most 150 queries for the same name. This flaw allows an off-path attacker on the network to substantially reduce the number of attempts that it would have to perform to forge a reply and have it accepted by dnsmasq. This issue is mentioned in the "Birthday Attacks" section of RFC5452. If chained with CVE-2020-25684, the attack complexity of a successful attack is reduced. The highest threat from this vulnerability is to data integrity.	3.7	More Details
CVE-2020-4889	IBM Spectrum Scale 5.0.0 through 5.0.5.4 and 5.1.0 could allow a local user to poison log files which could impact support and development efforts. IBM X-Force ID: 190971.	3.3	More Details
CVE-2021-2123	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. 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 read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N).	3.2	More Details
CVE-2021-2045	Vulnerability in the Oracle Text component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Oracle Text. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Text. CVSS 3.1 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L).	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2019	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.19 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 read access to a subset of MySQL Server 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-2021-1996	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 and 12.1.3.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. 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 WebLogic Server accessible data. CVSS 3.1 Base Score 2.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N).	2.4	More Details
CVE-2021-2000	Vulnerability in the Unified Audit component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having SYS Account privilege with network access via Oracle Net to compromise Unified Audit. 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 Unified Audit accessible data. CVSS 3.1 Base Score 2.4 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N).	2.4	More Details
CVE-2021-2042	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 and prior. Easily exploitable 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 read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).	2.3	More Details
CVE-2020-5481	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5494	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5493	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5492	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5495	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5490	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5489	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5488	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5491	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5478	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5480	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5479	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5486	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5477	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5476	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5475	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5474	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5473	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5472	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5471	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5470	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5469	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5487	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5485	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5482	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5460	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5452	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5453	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5454	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5455	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5456	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5457	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5458	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5459	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5461	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5450	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5484	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5462	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5463	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5464	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5465	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5466	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5467	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5483	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5451	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5449	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5429	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5438	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5430	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5431	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5432	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5433	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5468	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5435	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5436	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5437	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5439	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5448	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5440	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5441	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5442	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5443	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5444	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5445	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5446	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5447	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5434	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28290	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-35310	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none NOTE: This is disputed by the vendor; "We have no records of contact with the original reporter, and have not been able to reproduce any issue.	N/A	More Details
CVE-2020-13187	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2019-11305	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019. Notes: none	N/A	More Details
CVE-2019-11306	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019. Notes: none	N/A	More Details
CVE-2019-11307	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-11308	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019. Notes: none	N/A	More Details
CVE-2019-11309	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019. Notes: none	N/A	More Details
CVE-2019-11310	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019. Notes: none	N/A	More Details
CVE-2019-11311	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019. Notes: none	N/A	More Details
CVE-2019-11312	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019. Notes: none	N/A	More Details
CVE-2019-11313	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019. Notes: none	N/A	More Details
CVE-2019-11314	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019. Notes: none	N/A	More Details
CVE-2019-11315	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019. Notes: none	N/A	More Details
CVE-2019-11316	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-11317	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019. Notes: none	N/A	More Details
CVE-2020-13188	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13203	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13189	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13190	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13191	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13192	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13193	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13194	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13195	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13196	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13197	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13198	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13199	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13200	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13201	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2019-11304	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019. Notes: none	N/A	More Details
CVE-2019-11302	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-11301	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019. Notes: none	N/A	More Details
CVE-2019-11300	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019. Notes: none	N/A	More Details
CVE-2020-28488	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2020-28492	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA	N/A	More Details
CVE-2018-10330	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2018. Notes: none	N/A	More Details
CVE-2018-10331	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2018. Notes: none	N/A	More Details
CVE-2018-10332	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2018. Notes: none	N/A	More Details
CVE-2018-10333	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2018. Notes: none	N/A	More Details
CVE-2018-10334	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2018. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-10335	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2018. Notes: none	N/A	More Details
CVE-2018-10336	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2018. Notes: none	N/A	More Details
CVE-2018-10337	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2018. Notes: none	N/A	More Details
CVE-2018-10338	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2018. Notes: none	N/A	More Details
CVE-2018-10339	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2018. Notes: none	N/A	More Details
CVE-2018-10340	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2018. Notes: none	N/A	More Details
CVE-2018-10341	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2018. Notes: none	N/A	More Details
CVE-2018-10342	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2018. Notes: none	N/A	More Details
CVE-2018-10343	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2018. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-10344	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2018. Notes: none	N/A	More Details
CVE-2018-10345	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2018. Notes: none	N/A	More Details
CVE-2018-10346	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2018. Notes: none	N/A	More Details
CVE-2018-10347	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2018. Notes: none	N/A	More Details
CVE-2018-10348	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2018. Notes: none	N/A	More Details
CVE-2018-10349	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2018. Notes: none	N/A	More Details
CVE-2019-11295	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019. Notes: none	N/A	More Details
CVE-2019-11296	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019. Notes: none	N/A	More Details
CVE-2019-11297	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-11298	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019. Notes: none	N/A	More Details
CVE-2019-11299	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019. Notes: none	N/A	More Details
CVE-2020-13202	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13204	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28326	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28311	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28298	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28299	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28300	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28301	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28302	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28303	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28304	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28305	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28306	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28307	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28308	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28309	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28310	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28312	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13205	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28313	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28314	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28315	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28316	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28317	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28318	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28319	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28320	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28321	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28322	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28323	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28324	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28325	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28297	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28296	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28295	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28294	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13206	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13207	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13208	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13209	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13210	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13211	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13212	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13213	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13214	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13215	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13216	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13217	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13218	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13219	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13220	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-13221	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13222	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-17524	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2020-28284	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28285	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28286	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28287	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28288	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28289	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28291	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28292	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-28293	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2019-11303	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019. Notes: none	N/A	More Details