SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 27 October 2021

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-35652	Vulnerability in the Essbase Administration Services product of Oracle Essbase (component: EAS Console). The supported versions that are affected are Prior to 11.1.2.4.046 and Prior to 21.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Essbase Administration Services. While the vulnerability is in Essbase Administration Services, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Essbase Administration Services. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	10.0	More Details
CVE-2021-41873	Penguin Aurora TV Box 41502 is a high-end network HD set-top box produced by Tencent Video and Skyworth Digital. An unauthorized access vulnerability exists in the Penguin Aurora Box. An attacker can use the vulnerability to gain unauthorized access to a specific link to remotely control the TV.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41163	Discourse is an open source platform for community discussion. In affected versions maliciously crafted requests could lead to remote code execution. This resulted from a lack of validation in subscribe_url values. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. To workaround the issue without updating, requests with a path starting /webhooks/aws path could be blocked at an upstream proxy.	10.0	More Details
CVE-2021-35617	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Coherence Container). 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 unauthenticated attacker with network access via IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2011-4119	caml-light <= 0.75 uses mktemp() insecurely, and also does unsafe things in /tmp during make install.	9.8	More Details
CVE-2011-2195	A flaw was found in WebSVN 2.3.2. Without prior authentication, if the 'allowDownload' option is enabled in config.php, an attacker can invoke the dl.php script and pass a well formed 'path' argument to execute arbitrary commands against the underlying operating system.	9.8	More Details
CVE-2021-42343	An issue was discovered in the Dask distributed package before 2021.10.0 for Python. Single machine Dask clusters started with dask.distributed.LocalCluster or dask.distributed.Client (which defaults to using LocalCluster) would mistakenly configure their respective Dask workers to listen on external interfaces (typically with a randomly selected high port) rather than only on localhost. A Dask cluster created using this method (when running on a machine that has an applicable port exposed) could be used by a sophisticated attacker to achieve remote code execution.	9.8	More Details
CVE-2021-20837	Movable Type 7 r.5002 and earlier (Movable Type 7 Series), Movable Type 6.8.2 and earlier (Movable Type 6 Series), Movable Type Advanced 7 r.5002 and earlier (Movable Type Advanced 7 Series), Movable Type Advanced 6.8.2 and earlier (Movable Type Advanced 6 Series), Movable Type Premium 1.46 and earlier, and Movable Type Premium Advanced 1.46 and earlier allow remote attackers to execute arbitrary OS commands via unspecified vectors. Note that all versions of Movable Type 4.0 or later including unsupported (End-of-Life, EOL) versions are also affected by this vulnerability.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41035	In Eclipse Openj9 before version 0.29.0, the JVM does not throw IllegalAccessError for MethodHandles that invoke inaccessible interface methods.	9.8	More Details
CVE-2021-40865	An Unsafe Deserialization vulnerability exists in the worker services of the Apache Storm supervisor server allowing pre-auth Remote Code Execution (RCE). Apache Storm 2.2.x users should upgrade to version 2.2.1 or 2.3.0. Apache Storm 2.1.x users should upgrade to version 2.1.1. Apache Storm 1.x users should upgrade to version 1.2.4	9.8	More Details
CVE-2021-38294	A Command Injection vulnerability exists in the getTopologyHistory service of the Apache Storm 2.x prior to 2.2.1 and Apache Storm 1.x prior to 1.2.4. A specially crafted thrift request to the Nimbus server allows Remote Code Execution (RCE) prior to authentication.	9.8	More Details
CVE-2021-40371	Gridpro Request Management for Windows Azure Pack before 2.0.7912 allows Directory Traversal for remote code execution, as demonstrated by ..\\ in a scriptName JSON value to ServiceManagerTenant/GetVisibilityMap.	9.8	More Details
CVE-2021-42258	BQE BillQuick Web Suite 2018 through 2021 before 22.0.9.1 allows SQL injection for unauthenticated remote code execution, as exploited in the wild in October 2021 for ransomware installation. SQL injection can, for example, use the txtID (aka username) parameter. Successful exploitation can include the ability to execute arbitrary code as MSSQLSERVER$ via xp_cmdshell.	9.8	More Details
CVE-2020-28960	Chichen Tech CMS v1.0 was discovered to contain multiple SQL injection vulnerabilities in the file product_list.php via the id and cid parameters.	9.8	More Details
CVE-2020-23037	Portable Ltd Playable v9.18 contains a code injection vulnerability in the filename parameter, which allows attackers to execute arbitrary web scripts or HTML via a crafted POST request.	9.8	More Details
CVE-2021-42169	The Simple Payroll System with Dynamic Tax Bracket in PHP using SQLite Free Source Code (by: oretnom23) is vulnerable from remote SQL-Injection-Bypass-Authentication for the admin account. The parameter (username) from the login form is not protected correctly and there is no security and escaping from malicious payloads.	9.8	More Details
CVE-2021-41745	ShowDoc 2.8.3 ihas a file upload vulnerability, where attackers can use the vulnerability to obtain server permissions.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41744	All versions of yongyou PLM are affected by a command injection issue. UFIDA PLM (Product Life Cycle Management) is a strategic management method. It applies a series of enterprise application systems to support the entire process from conceptual design to the end of product life, and the collaborative creation, distribution, application and management of product information across organizations. Yonyou PLM uses jboss by default, and you can access the management control background without authorization An attacker can use this vulnerability to gain server permissions.	9.8	More Details
CVE-2021-36357	An issue was discovered in OpenPOWER 2.6 firmware. unpack_timestamp() calls le32_to_cpu() for endian conversion of a uint16_t "year" value, resulting in a type mismatch that can truncate a higher integer value to a smaller one, and bypass a timestamp check. The fix is to use the right endian conversion function.	9.8	More Details
CVE-2021-21748	ZTE MF971R product has two stack-based buffer overflow vulnerabilities. An attacker could exploit the vulnerabilities to execute arbitrary code.	9.8	More Details
CVE-2021-21749	ZTE MF971R product has two stack-based buffer overflow vulnerabilities. An attacker could exploit the vulnerabilities to execute arbitrary code.	9.8	More Details
CVE-2021-42740	The shell-quote package before 1.7.3 for Node.js allows command injection. An attacker can inject unescaped shell metacharacters through a regex designed to support Windows drive letters. If the output of this package is passed to a real shell as a quoted argument to a command with exec(), an attacker can inject arbitrary commands. This is because the Windows drive letter regex character class is {A-z] instead of the correct {A-Za-z]. Several shell metacharacters exist in the space between capital letter Z and lower case letter a, such as the backtick character.	9.8	More Details
CVE-2020-27304	The CivetWeb web library does not validate uploaded filepaths when running on an OS other than Windows, when using the built-in HTTP form-based file upload mechanism, via the mg_handle_form_request API. Web applications that use the file upload form handler, and use parts of the user-controlled filename in the output path, are susceptible to directory traversal	9.8	More Details
CVE-2021-38477	There are multiple API function codes that permit reading and writing data to or from files and directories, which could lead to the manipulation and/or the deletion of files.	9.8	More Details
CVE-2021-37371	Online Student Admission System 1.0 is affected by an unauthenticated SQL injection bypass vulnerability in /admin/login.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38449	Some API functions permit by-design writing or copying data into a given buffer. Since the client controls these parameters, an attacker could rewrite the memory in any location of the affected product.	9.8	More Details
CVE-2021-38457	The server permits communication without any authentication procedure, allowing the attacker to initiate a session with the server without providing any form of authentication.	9.8	More Details
CVE-2021-24884	The Formidable Form Builder WordPress plugin before 4.09.05 allows to inject certain HTML Tags like <audio>,<video>,<img>,<a> and<button>.This could allow an unauthenticated, remote attacker to exploit a HTML-injection byinjecting a malicous link. The HTML-injection may trick authenticated users to follow the link. If the Link gets clicked, Javascript code can be executed. The vulnerability is due to insufficient sanitization of the "data-frmverify" tag for links in the web-based entry inspection page of affected systems. A successful exploitation incomibantion with CSRF could allow the attacker to perform arbitrary actions on an affected system with the privileges of the user. These actions include stealing the users account by changing their password or allowing attackers to submit their own code through an authenticated user resulting in Remote Code Execution. If an authenticated user who is able to edit Wordpress PHP Code in any kind, clicks the malicious link, PHP code can be edited.	9.6	More Details
CVE-2021-38453	Some API functions allow interaction with the registry, which includes reading values as well as data modification.	9.1	More Details
CVE-2021-34584	Crafted web server requests can be utilised to read partial stack or heap memory or may trigger a denial-of- service condition due to a crash in the CODESYS V2 web server prior to V1.1.9.22.	9.1	More Details
CVE-2021-42766	The Proof-of-Stake (PoS) Ethereum consensus protocol through 2021-10-19 allows an adversary to cause a denial of service (long-range consensus chain reorganizations), even when this adversary has little stake and cannot influence network message propagation. This can cause a protocol stall, or an increase in the profits of individual validators.	9.1	More Details
CVE-2021-42764	The Proof-of-Stake (PoS) Ethereum consensus protocol through 2021-10-19 allows an adversary to cause a denial of service (delayed consensus decisions), and also increase the profits of individual validators, via short-range reorganizations of the underlying consensus chain.	9.1	More Details
CVE-2021-38469	Many of the services used by the affected product do not specify full paths for the DLLs they are loading. An attacker can exploit the uncontrolled search path by implanting their own DLL near the affected product’s binaries, thus hijacking the loaded DLL.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38471	There are multiple API function codes that permit data writing to any file, which may allow an attacker to modify existing files or create new files.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-25970	Camaleon CMS 0.1.7 to 2.6.0 doesn't terminate the active session of the users, even after the admin changes the user's password. A user that was already logged in, will still have access to the application even after the password was changed.	8.8	More Details
CVE-2021-34864	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.1.3 (49160). An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the WinAppHelper component. The issue results from the lack of proper access control. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13543.	8.8	More Details
CVE-2020-23043	Tran Tu Air Sender v1.0.2 was discovered to contain an arbitrary file upload vulnerability in the upload module. This vulnerability allows attackers to execute arbitrary code via a crafted file.	8.8	More Details
CVE-2021-34859	This vulnerability allows remote attackers to execute arbitrary code on affected installations of TeamViewer 15.16.8.0. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of TVS files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13697.	8.8	More Details
CVE-2021-37372	Online Student Admission System 1.0 is affected by an insecure file upload vulnerability. A low privileged user can upload malicious PHP files by updating their profile image to gain remote code execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41146	qutebrowser is an open source keyboard-focused browser with a minimal GUI. Starting with qutebrowser v1.7.0, the Windows installer for qutebrowser registers a `qutebrowserurl:` URL handler. With certain applications, opening a specially crafted `qutebrowserurl:...` URL can lead to execution of qutebrowser commands, which in turn allows arbitrary code execution via commands such as `:spawn` or `:debug-pyeval`. Only Windows installs where qutebrowser is registered as URL handler are affected. The issue has been fixed in qutebrowser v2.4.0. The fix also adds additional hardening for potential similar issues on Linux (by adding the new --untrusted-args flag to the .desktop file), though no such vulnerabilities are known.	8.8	More Details
CVE-2021-41185	Mycodo is an environmental monitoring and regulation system. An exploit in versions prior to 8.12.7 allows anyone with access to endpoints to download files outside the intended directory. A patch has been applied and a release made. Users should upgrade to version 8.12.7. As a workaround, users may manually apply the changes from the fix commit.	8.8	More Details
CVE-2021-42840	SuiteCRM before 7.11.19 allows remote code execution via the system settings Log File Name setting. In certain circumstances involving admin account takeover, logger_file_name can refer to an attacker-controlled PHP file under the web root, because only the all-lowercase PHP file extensions were blocked. NOTE: this issue exists because of an incomplete fix for CVE-2020-28328.	8.8	More Details
CVE-2021-24487	The St-Daily-Tip WordPress plugin through 4.7 does not have any CSRF check in place when saving its 'Default Text to Display if no tips' setting, and was also lacking sanitisation as well as escaping before outputting it the page. This could allow attacker to make logged in administrators set a malicious payload in it, leading to a Stored Cross-Site Scripting issue	8.8	More Details
CVE-2021-2137	Vulnerability in the Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Policy Framework). Supported versions that are affected are 13.4.0.0 and 13.5.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in takeover of Enterprise Manager Base Platform. 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-2021-39321	Version 3.3.23 of the Sassy Social Share WordPress plugin is vulnerable to PHP Object Injection via the wp_ajax_heateor_sss_import_config AJAX action due to deserialization of unvalidated user supplied inputs via the import_config function found in the ~/admin/class-sassy-social-share-admin.php file. This can be exploited by underprivileged authenticated users due to a missing capability check on the import_config function.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41178	Nextcloud is an open-source, self-hosted productivity platform. Prior to versions 20.0.13, 21.0.5, and 22.2.0, a file traversal vulnerability makes an attacker able to download arbitrary SVG images from the host system, including user provided files. This could also be leveraged into a XSS/phishing attack, an attacker could upload a malicious SVG file that mimics the Nextcloud login form and send a specially crafted link to victims. The XSS risk here is mitigated due to the fact that Nextcloud employs a strict Content-Security-Policy disallowing execution of arbitrary JavaScript. It is recommended that the Nextcloud Server be upgraded to 20.0.13, 21.0.5 or 22.2.0. There are no known workarounds aside from upgrading.	8.8	More Details
CVE-2021-20120	The administration web interface for the Arris Surfboard SB8200 lacks any protections against cross-site request forgery attacks. This means that an attacker could make configuration changes (such as changing the administrative password) without the consent of the user.	8.8	More Details
CVE-2021-34861	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2020 1.01rc001 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the webproc endpoint, which listens on TCP port 80 by default. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-12104.	8.8	More Details
CVE-2021-34856	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.1.3 (49160). An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the virtio-gpu virtual device. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13581.	8.8	More Details
CVE-2021-41790	An issue was discovered in Hyland org.alfresco:alfresco-content-services through 7.0.1.2. Script Action execution allows executing scripts uploaded outside of the Data Dictionary. This could allow a logged-in attacker to execute arbitrary code inside a sandboxed environment.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34863	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2020 1.01rc001 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the var:page parameter provided to the webproc endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-13271.	8.8	More Details
CVE-2020-28967	FlashGet v1.9.6 was discovered to contain a buffer overflow in the 'current path directory' function. This vulnerability allows attackers to elevate local process privileges via overwriting the registers.	8.8	More Details
CVE-2021-34857	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.1.3 (49160). An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13601.	8.8	More Details
CVE-2021-34862	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2020 1.01rc001 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the var:menu parameter provided to the webproc endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-13270.	8.8	More Details
CVE-2021-34362	A command injection vulnerability has been reported to affect QNAP device running Media Streaming add-on. If exploited, this vulnerability allow remote attackers to run arbitrary commands. We have already fixed this vulnerability in the following versions of Media Streaming add-on: QTS 5.0.0: Media Streaming add-on 500.0.0.3 (2021/08/20) and later QTS 4.5.4: Media Streaming add-on 500.0.0.3 (2021/08/20) and later QTS 4.3.6: Media Streaming add-on 430.1.8.12 (2021/08/20) and later QTS 4.3.3: Media Streaming add-on 430.1.8.12 (2021/09/29) and later QuTS-Hero 5.0.0: Media Streaming add-on 500.0.0.3 (2021/08/20) and later	8.7	More Details
CVE-2021-23452	This affects all versions of package x-assign. The global proto object can be polluted using the __proto__ object.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40527	Exposure of senstive information to an unauthorised actor in the "com.onepeloton.erlich" mobile application up to and including version 1.7.22 allows a remote attacker to access developer files stored in an AWS S3 bucket, by reading credentials stored in plain text within the mobile application.	8.6	More Details
CVE-2020-11303	Accepting AMSDU frames with mismatched destination and source address can lead to information disclosure in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	8.6	More Details
CVE-2021-41145	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. FreeSWITCH prior to version 1.10.7 is susceptible to Denial of Service via SIP flooding. When flooding FreeSWITCH with SIP messages, it was observed that after a number of seconds the process was killed by the operating system due to memory exhaustion. By abusing this vulnerability, an attacker is able to crash any FreeSWITCH instance by flooding it with SIP messages, leading to Denial of Service. The attack does not require authentication and can be carried out over UDP, TCP or TLS. This issue was patched in version 1.10.7.	8.6	More Details
CVE-2021-35651	Vulnerability in the Essbase Administration Services product of Oracle Essbase (component: EAS Console). The supported versions that are affected are Prior to 11.1.2.4.046 and Prior to 21.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Essbase Administration Services. While the vulnerability is in Essbase Administration Services, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Essbase Administration Services accessible data as well as unauthorized update, insert or delete access to some of Essbase Administration Services accessible data. CVSS 3.1 Base Score 8.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N).	8.5	More Details
CVE-2021-1913	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	8.4	More Details
CVE-2021-1984	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1932	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	8.4	More Details
CVE-2021-1917	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables	8.4	More Details
CVE-2021-1949	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details
CVE-2021-1983	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	8.4	More Details
CVE-2021-30316	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	8.4	More Details
CVE-2021-30315	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto	8.4	More Details
CVE-2021-1985	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	8.4	More Details
CVE-2021-30256	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT	8.4	More Details
CVE-2021-30257	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT	8.4	More Details
CVE-2021-30258	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30288	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable 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	8.4	More Details
CVE-2021-30291	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	8.4	More Details
CVE-2021-30292	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	8.4	More Details
CVE-2021-30297	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	8.4	More Details
CVE-2021-30305	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	8.4	More Details
CVE-2021-30306	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	8.4	More Details
CVE-2021-2461	Vulnerability in the Oracle Communications Interactive Session Recorder product of Oracle Communications (component: Provision API). The supported version that is affected is 6.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Communications Interactive Session Recorder. While the vulnerability is in Oracle Communications Interactive Session Recorder, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Communications Interactive Session Recorder accessible data as well as unauthorized read access to a subset of Oracle Communications Interactive Session Recorder accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Communications Interactive Session Recorder. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L).	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38461	The affected product uses a hard-coded blowfish key for encryption/decryption processes. The key can be easily extracted from binaries.	8.2	More Details
CVE-2021-35599	Vulnerability in the Zero Downtime DB Migration to Cloud component of Oracle Database Server. The supported version that is affected is 21c. Easily exploitable vulnerability allows high privileged attacker having Local Logon privilege with logon to the infrastructure where Zero Downtime DB Migration to Cloud executes to compromise Zero Downtime DB Migration to Cloud. While the vulnerability is in Zero Downtime DB Migration to Cloud, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Zero Downtime DB Migration to Cloud. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details
CVE-2021-0870	In RW_SetActivatedTagType of rw_main.cc, there is possible memory corruption due to a race condition. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-192472262	8.1	More Details
CVE-2021-34595	A crafted request with invalid offsets may cause an out-of-bounds read or write access in CODESYS V2 Runtime Toolkit 32 Bit full and PLCWinNT prior to versions V2.4.7.56, resulting in a denial-of-service condition or local memory overwrite.	8.1	More Details
CVE-2021-35566	Vulnerability in the Oracle Applications Manager product of Oracle E-Business Suite (component: Diagnostics). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Applications Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Applications Manager accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35570	Vulnerability in the Oracle Mobile Field Service product of Oracle E-Business Suite (component: Admin UI). 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 Mobile Field Service. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Mobile Field Service accessible data as well as unauthorized access to critical data or complete access to all Oracle Mobile Field Service accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-35563	Vulnerability in the Oracle Shipping Execution product of Oracle E-Business Suite (component: Workflow Events). Supported versions that are affected are 12.2.6-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Shipping Execution. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Shipping Execution accessible data as well as unauthorized access to critical data or complete access to all Oracle Shipping Execution accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-35562	Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Work Provider Site Level Administration). 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 Universal Work Queue. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Universal Work Queue accessible data as well as unauthorized access to critical data or complete access to all Oracle Universal Work Queue accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-41177	Nextcloud is an open-source, self-hosted productivity platform. Prior to versions 20.0.13, 21.0.5, and 22.2.0, Nextcloud Server did not implement a database backend for rate-limiting purposes. Any component of Nextcloud using rate-limits (as as `AnonRateThrottle` or `UserRateThrottle`) was thus not rate limited on instances not having a memory cache backend configured. In the case of a default installation, this would notably include the rate-limits on the two factor codes. It is recommended that the Nextcloud Server be upgraded to 20.0.13, 21.0.5, or 22.2.0. As a workaround, enable a memory cache backend in `config.php`.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26607	An Improper input validation in execDefaultBrowser method of NEXACRO17 allows a remote attacker to execute arbitrary command on affected systems.	8.1	More Details
CVE-2021-35543	Vulnerability in the PeopleSoft Enterprise CC Common Application Objects product of Oracle PeopleSoft (component: Activity Guide Composer). 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 CC Common Application Objects. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise CC Common Application Objects accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise CC Common Application Objects accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-38459	The data of a network capture of the initial handshake phase can be used to authenticate at a SYSDBA level. If a specific .exe is not restarted often, it is possible to access the needed handshake packets between admin/client connections. Using the SYSDBA permission, an attacker can change user passwords or delete the database.	8.1	More Details
CVE-2021-2482	Vulnerability in the Oracle Payables product of Oracle E-Business Suite (component: Invoice Approvals). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Payables. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Payables accessible data as well as unauthorized access to critical data or complete access to all Oracle Payables accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-29873	IBM Flash System 900 could allow an authenticated attacker to obtain sensitive information and cause a denial of service due to a restricted shell escape vulnerability. IBM X-Force ID: 206229.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35536	Vulnerability in the Oracle Deal Management product of Oracle E-Business Suite (component: Miscellaneous). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Deal Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Deal Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Deal Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-38481	The scheduler service running on a specific TCP port enables the user to start and stop jobs. There is no sanitation of the supplied JOB ID provided to the function. An attacker may send a malicious payload that can enable the user to execute another SQL expression by sending a specific string.	8.1	More Details
CVE-2021-2474	Vulnerability in the Oracle Web Analytics product of Oracle E-Business Suite (component: Admin). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Web Analytics. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Web Analytics accessible data as well as unauthorized access to critical data or complete access to all Oracle Web 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-2019-3556	HHVM supports the use of an "admin" server which accepts administrative requests over HTTP. One of those request handlers, dump-pcre-cache, can be used to output cached regular expressions from the current execution context into a file. The handler takes a parameter which specifies where on the filesystem to write this data. The parameter is not validated, allowing a malicious user to overwrite arbitrary files where the user running HHVM has write access. This issue affects HHVM versions prior to 4.56.2, all versions between 4.57.0 and 4.78.0, as well as 4.79.0, 4.80.0, 4.81.0, 4.82.0, and 4.83.0.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2483	Vulnerability in the Oracle Content Manager product of Oracle E-Business Suite (component: Content Item Manager). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Content Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Content Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Content Manager accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2484	Vulnerability in the Oracle Operations Intelligence product of Oracle E-Business Suite (component: BIS Operations Intelligence). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Operations Intelligence. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Operations Intelligence accessible data as well as unauthorized access to critical data or complete access to all Oracle Operations Intelligence accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-2485	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: Quotes). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Trade Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Trade Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2021-35585	Vulnerability in the Oracle Incentive Compensation product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Incentive Compensation. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Incentive Compensation accessible data as well as unauthorized access to critical data or complete access to all Oracle Incentive Compensation accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39225	Nextcloud is an open-source, self-hosted productivity platform. A missing permission check in Nextcloud Deck before 1.2.9, 1.4.5 and 1.5.3 allows another authenticated users to access Deck cards of another user. It is recommended that the Nextcloud Deck App is upgraded to 1.2.9, 1.4.5 or 1.5.3. There are no known workarounds aside from upgrading.	8.1	More Details
CVE-2021-35499	The Web Reporting component of TIBCO Software Inc.'s TIBCO Nimbus contains easily exploitable Stored Cross Site Scripting (XSS) vulnerabilities that allow a low privileged attacker to social engineer a legitimate user with network access to execute scripts targeting the affected system or the victim's local system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO Nimbus: versions 10.4.0 and below.	8.0	More Details
CVE-2021-38473	The affected product’s code base doesn’t properly control arguments for specific functions, which could lead to a stack overflow.	8.0	More Details
CVE-2021-42539	The affected product is vulnerable to a missing permission validation on system backup restore, which could lead to account take over and unapproved settings change.	8.0	More Details
CVE-2021-42538	The affected product is vulnerable to a parameter injection via passphrase, which enables the attacker to supply uncontrolled input.	8.0	More Details
CVE-2021-38485	The affected product is vulnerable to improper input validation in the restore file. This enables an attacker to provide malicious config files to replace any file on disk.	8.0	More Details
CVE-2021-38465	The webinstaller is a Golang web server executable that enables the generation of an Auvesy image agent. Resource consumption can be achieved by generating large amounts of installations, which are then saved without limitation in the temp folder of the webinstaller executable.	8.0	More Details
CVE-2021-42540	The affected product is vulnerable to a unsanitized extract folder for system configuration. A low-privileged user can leverage this logic to overwrite the settings and other key functionality.	8.0	More Details
CVE-2021-42097	GNU Mailman before 2.1.35 may allow remote Privilege Escalation. A csrf_token value is not specific to a single user account. An attacker can obtain a value within the context of an unprivileged user account, and then use that value in a CSRF attack against an admin (e.g., for account takeover).	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-23050	TAO Open Source Assessment Platform v3.3.0 RC02 was discovered to contain a HTML injection vulnerability in the userFirstName parameter of the user account input field. This vulnerability allows attackers to execute phishing attacks, external redirects, and arbitrary code.	8.0	More Details
CVE-2021-42536	The affected product is vulnerable to a disclosure of peer username and password by allowing all users access to read global variables.	8.0	More Details
CVE-2021-42542	The affected product is vulnerable to directory traversal due to mishandling of provided backup folder structure.	8.0	More Details
CVE-2021-42108	Unnecessary privilege vulnerabilities in the Web Console of Trend Micro Apex One, Apex One as a Service and Worry-Free Business Security 10.0 SP1 could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2021-42102	An uncontrolled search path element vulnerabilities in Trend Micro Apex One and Apex One as a Service agents could allow a local attacker to escalate privileges on affected installations. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2020-28963	Passcovery Co. Ltd ZIP Password Recovery v3.70.69.0 was discovered to contain a buffer overflow via the decompress function.	7.8	More Details
CVE-2021-42012	A stack-based buffer overflow vulnerability in Trend Micro Apex One, Apex One as a Service and Worry-Free Business Security 10.0 SP1 could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2021-38260	NXP MCUXpresso SDK v2.7.0 was discovered to contain a buffer overflow in the function USB_HostParseDeviceConfigurationDescriptor().	7.8	More Details
CVE-2021-38258	NXP MCUXpresso SDK v2.7.0 was discovered to contain a buffer overflow in the function USB_HostProcessCallback().	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34854	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.1.3 (49160). An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. The issue results from the lack of proper validation of user-supplied data, which can result in an uncontrolled memory allocation. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13544.	7.8	More Details
CVE-2021-42104	Unnecessary privilege vulnerabilities in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1 and Worry-Free Business Security Services could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but not identical to CVE-2021-42105, 42106 and 42107.	7.8	More Details
CVE-2021-42101	An uncontrolled search path element vulnerabilities in Trend Micro Apex One and Apex One as a Service could allow a local attacker to escalate privileges on affected installations. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar but not identical to CVE-2021-42103.	7.8	More Details
CVE-2021-30359	The Harmony Browse and the SandBlast Agent for Browsers installers must have admin privileges to execute some steps during the installation. Because the MS Installer allows regular users to repair their installation, an attacker running an installer before 90.08.7405 can start the installation repair and place a specially crafted binary in the repair folder, which runs with the admin privileges.	7.8	More Details
CVE-2021-42103	An uncontrolled search path element vulnerabilities in Trend Micro Apex One and Apex One as a Service could allow a local attacker to escalate privileges on affected installations. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar but not identical to CVE-2021-42101.	7.8	More Details
CVE-2021-42106	Unnecessary privilege vulnerabilities in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1 and Worry-Free Business Security Services could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but not identical to CVE-2021-42104, 42105 and 42107.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42105	Unnecessary privilege vulnerabilities in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1 and Worry-Free Business Security Services could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but not identical to CVE-2021-42104, 42106 and 42107.	7.8	More Details
CVE-2021-42107	Unnecessary privilege vulnerabilities in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1 and Worry-Free Business Security Services could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but not identical to CVE-2021-42104, 42105 and 42106.	7.8	More Details
CVE-2021-37363	An Insecure Permissions issue exists in Gestionale Open 11.00.00. A low privilege account is able to rename the mysqld.exe file located in bin folder and replace with a malicious file that would connect back to an attacking computer giving system level privileges (nt authority\system) due to the service running as Local System. While a low privilege user is unable to restart the service through the application, a restart of the computer triggers the execution of the malicious file. The application also have unquoted service path issues.	7.8	More Details
CVE-2021-42011	An incorrect permission assignment vulnerability in Trend Micro Apex One and Apex One as a Service could allow a local attacker to load a DLL with escalated privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2021-42771	Babel.Locale in Babel before 2.9.1 allows attackers to load arbitrary locale .dat files (containing serialized Python objects) via directory traversal, leading to code execution.	7.8	More Details
CVE-2021-0652	In VectorDrawable::VectorDrawable of VectorDrawable.java, there is a possible way to introduce a memory corruption due to sharing of not thread-safe objects. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-185178568	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35538	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.28. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. Note: This vulnerability does not apply to Windows systems. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	7.8	More Details
CVE-2021-21703	In PHP versions 7.3.x up to and including 7.3.31, 7.4.x below 7.4.25 and 8.0.x below 8.0.12, when running PHP FPM SAPI with main FPM daemon process running as root and child worker processes running as lower-privileged users, it is possible for the child processes to access memory shared with the main process and write to it, modifying it in a way that would cause the root process to conduct invalid memory reads and writes, which can be used to escalate privileges from local unprivileged user to the root user.	7.8	More Details
CVE-2021-0483	In multiple methods of AAudioService, there is a possible use-after-free due to a race condition. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-153358911	7.8	More Details
CVE-2020-36485	Portable Ltd Playable v9.18 was discovered to contain an arbitrary file upload vulnerability in the filename parameter of the upload module. This vulnerability allows attackers to execute arbitrary code via a crafted JPEG file.	7.8	More Details
CVE-2021-37364	OpenClinic GA 5.194.18 is affected by Insecure Permissions. By default the Authenticated Users group has the modify permission to openclinic folders/files. A low privilege account is able to rename mysqld.exe or tomcat8.exe files located in bin folders and replace with a malicious file that would connect back to an attacking computer giving system level privileges (nt authority\system) due to the service running as Local System. While a low privilege user is unable to restart the service through the application, a restart of the computer triggers the execution of the malicious file. The application also have unquoted service path issues.	7.8	More Details
CVE-2021-41078	Nameko through 2.13.0 can be tricked into performing arbitrary code execution when deserializing the config file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0705	In sanitizeSbn of NotificationManagerService.java, there is a possible way to keep service running in foreground and keep granted permissions due to Bypass of Background Service Restrictions. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-10Android ID: A-185388103	7.8	More Details
CVE-2021-40343	An issue was discovered in Nagios XI 5.8.5. Insecure file permissions on the nagios_unbundler.py file allow the nagios user to elevate their privileges to the root user.	7.8	More Details
CVE-2020-28969	Aplioxio PDF ShapingUp 5.0.0.139 contains a buffer overflow which allows attackers to cause a denial of service (DoS) via a crafted PDF file.	7.8	More Details
CVE-2021-1529	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges.	7.8	More Details
CVE-2021-0936	In acc_read of f_accessory.c, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-173789633References: Upstream kernel	7.8	More Details
CVE-2021-1959	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.8	More Details
CVE-2021-0708	In runDumpHeap of ActivityManagerShellCommand.java, there is a possible deletion of system files due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-183262161	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35653	Vulnerability in the Essbase Administration Services product of Oracle Essbase (component: EAS Console). The supported versions that are affected are Prior to 11.1.2.4.046 and Prior to 21.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Essbase Administration Services. While the vulnerability is in Essbase Administration Services, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Essbase Administration Services accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	7.7	More Details
CVE-2021-35662	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2021-41167	modern-async is an open source JavaScript tooling library for asynchronous operations using async/await and promises. In affected versions a bug affecting two of the functions in this library: forEachSeries and forEachLimit. They should limit the concurrency of some actions but, in practice, they don't. Any code calling these functions will be written thinking they would limit the concurrency but they won't. This could lead to potential security issues in other projects. The problem has been patched in 1.0.4. There is no workaround.	7.5	More Details
CVE-2021-42765	The Proof-of-Stake (PoS) Ethereum consensus protocol through 2021-10-19 allows an adversary to leverage network delay to cause a denial of service (indefinite stalling of consensus decisions).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37624	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.10.7, FreeSWITCH does not authenticate SIP MESSAGE requests, leading to spam and message spoofing. By default, SIP requests of the type MESSAGE (RFC 3428) are not authenticated in the affected versions of FreeSWITCH. MESSAGE requests are relayed to SIP user agents registered with the FreeSWITCH server without requiring any authentication. Although this behaviour can be changed by setting the `auth-messages` parameter to `true`, it is not the default setting. Abuse of this security issue allows attackers to send SIP MESSAGE messages to any SIP user agent that is registered with the server without requiring authentication. Additionally, since no authentication is required, chat messages can be spoofed to appear to come from trusted entities. Therefore, abuse can lead to spam and enable social engineering, phishing and similar attacks. This issue is patched in version 1.10.7. Maintainers recommend that this SIP message type is authenticated by default so that FreeSWITCH administrators do not need to be explicitly set the `auth-messages` parameter. When following such a recommendation, a new parameter can be introduced to explicitly disable authentication.	7.5	More Details
CVE-2021-35661	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35660	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2021-35659	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2021-35658	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35656	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2021-35654	Vulnerability in the Essbase Administration Services product of Oracle Essbase (component: EAS Console). The supported versions that are affected are Prior to 11.1.2.4.046 and Prior to 21.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Essbase Administration Services. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Essbase Administration Services. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2021-0630	In wifi driver, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05551397; Issue ID: ALPS05551397.	7.5	More Details
CVE-2021-0631	In wifi driver, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05551435; Issue ID: ALPS05551435.	7.5	More Details
CVE-2020-23040	Sky File v2.1.0 contains a directory traversal vulnerability in the FTP server which allows attackers to access sensitive data and files via 'null' path commands.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35657	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2021-41306	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to view private project and filter names via an Insecure Direct Object References (IDOR) vulnerability in the Average Time in Status Gadget. The affected versions are before version 8.13.12, and from version 8.14.0 before 8.20.0.	7.5	More Details
CVE-2021-23139	A null pointer vulnerability in Trend Micro Apex One and Worry-Free Business Security 10.0 SP1 could allow an attacker to crash the CGI program on affected installations.	7.5	More Details
CVE-2021-35572	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2021-34586	In the CODESYS V2 web server prior to V1.1.9.22 crafted web server requests may cause a Null pointer dereference in the CODESYS web server and may result in a denial-of-service condition.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35620	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2021-35560	Vulnerability in the Java SE product of Oracle Java SE (component: Deployment). The supported version that is affected is Java SE: 8u301. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).	7.5	More Details
CVE-2021-26609	A vulnerability was found in Mangboard(WordPress plugin). A SQL-Injection vulnerability was found in order_type parameter. The order_type parameter makes a SQL query using unfiltered data. This vulnerability allows a remote attacker to steal user information.	7.5	More Details
CVE-2021-42836	GJSON before 1.9.3 allows a ReDoS (regular expression denial of service) attack.	7.5	More Details
CVE-2020-23061	Dropouts Technologies LLP Super Backup v2.0.5 was discovered to contain an issue in the path parameter of the `list` and `download` module which allows attackers to perform a directory traversal via a change to the path variable to request the local list command.	7.5	More Details
CVE-2020-23038	Swift File Transfer Mobile v1.1.2 and below was discovered to contain an information disclosure vulnerability in the path parameter. This vulnerability is exploited via an error caused by including non-existent path environment variables.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22034	Releases prior to VMware vRealize Operations Tenant App 8.6 contain an Information Disclosure Vulnerability.	7.5	More Details
CVE-2021-30312	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2021-30310	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music	7.5	More Details
CVE-2021-30304	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity	7.5	More Details
CVE-2021-30302	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2021-1980	Possible buffer over read due to lack of length check while parsing beacon IE response 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-2021-1977	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music	7.5	More Details
CVE-2021-1936	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34585	In the CODESYS V2 web server prior to V1.1.9.22 crafted web server requests can trigger a parser error. Since the parser result is not checked under all conditions, a pointer dereference with an invalid address can occur. This leads to a denial of service situation.	7.5	More Details
CVE-2021-34593	In CODESYS V2 Runtime Toolkit 32 Bit full and PLCWinNT prior to versions V2.4.7.56 unauthenticated crafted invalid requests may result in several denial-of-service conditions. Running PLC programs may be stopped, memory may be leaked, or further communication clients may be blocked from accessing the PLC.	7.5	More Details
CVE-2021-35573	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2021-41307	Affected versions of Atlassian Jira Server and Data Center allow unauthenticated remote attackers to view the names of private projects and private filters via an Insecure Direct Object References (IDOR) vulnerability in the Workload Pie Chart Gadget. The affected versions are before version 8.13.12, and from version 8.14.0 before 8.20.0.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41105	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. When handling SRTP calls, FreeSWITCH prior to version 1.10.7 is susceptible to a DoS where calls can be terminated by remote attackers. This attack can be done continuously, thus denying encrypted calls during the attack. When a media port that is handling SRTP traffic is flooded with a specially crafted SRTP packet, the call is terminated leading to denial of service. This issue was reproduced when using the SDES key exchange mechanism in a SIP environment as well as when using the DTLS key exchange mechanism in a WebRTC environment. The call disconnection occurs due to line 6331 in the source file `switch_rtp.c`, which disconnects the call when the total number of SRTP errors reach a hard-coded threshold (100). By abusing this vulnerability, an attacker is able to disconnect any ongoing calls that are using SRTP. The attack does not require authentication or any special foothold in the caller's or the callee's network. This issue is patched in version 1.10.7.	7.5	More Details
CVE-2021-35583	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Windows). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2021-41305	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to view the names of private projects and filters via an Insecure Direct Object References (IDOR) vulnerability in the Average Number of Times in Status Gadget. The affected versions are before version 8.13.12..	7.5	More Details
CVE-2021-21744	ZTE MF971R product has a configuration file control vulnerability. An attacker could use this vulnerability to modify the configuration parameters of the device, causing some security functions of the device to be disabled.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35574	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2021-34583	Crafted web server requests may cause a heap-based buffer overflow and could therefore trigger a denial-of- service condition due to a crash in the CODESYS V2 web server prior to V1.1.9.22.	7.5	More Details
CVE-2021-38455	The affected product's OS Service does not verify any given parameter. A user can supply any type of parameter that will be passed to inner calls without checking the type of the parameter or the value.	7.3	More Details
CVE-2021-38467	A specific function code receives a raw pointer supplied by the user and deallocates this pointer. The user can then control what memory regions will be freed and cause use-after-free condition.	7.3	More Details
CVE-2021-38475	The database connection to the server is performed by calling a specific API, which could allow an unprivileged user to gain SYSDBA permissions.	7.3	More Details
CVE-2021-41127	Rasa is an open source machine learning framework to automate text-and voice-based conversations. In affected versions a vulnerability exists in the functionality that loads a trained model `tar.gz` file which allows a malicious actor to craft a `model.tar.gz` file which can overwrite or replace bot files in the bot directory. The vulnerability is fixed in Rasa 2.8.10. For users unable to update ensure that users do not upload untrusted model files, and restrict CLI or API endpoint access where a malicious actor could target a deployed Rasa instance.	7.3	More Details
CVE-2021-41175	Pi-hole's Web interface (based on AdminLTE) provides a central location to manage one's Pi-hole and review the statistics generated by FTLDNS. Prior to version 5.8, cross-site scripting is possible when adding a client via the groups-clients management page. This issue was patched in version 5.8.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38463	The affected product does not properly control the allocation of resources. A user may be able to allocate unlimited memory buffers using API functions.	7.3	More Details
CVE-2021-24769	The Permalink Manager Lite WordPress plugin before 2.2.13.1 does not validate and escape the orderby parameter before using it in a SQL statement in the Permalink Manager page, leading to a SQL Injection	7.2	More Details
CVE-2021-39352	The Catch Themes Demo Import WordPress plugin is vulnerable to arbitrary file uploads via the import functionality found in the ~/inc/CatchThemesDemoImport.php file, in versions up to and including 1.7, due to insufficient file type validation. This makes it possible for an attacker with administrative privileges to upload malicious files that can be used to achieve remote code execution.	7.2	More Details
CVE-2020-23045	Macrob7 Macs Framework Content Management System - 1.14f was discovered to contain a SQL injection vulnerability via the 'roleId' parameter of the `editRole` and `deletUser` modules.	7.2	More Details
CVE-2021-24774	The Check & Log Email WordPress plugin before 1.0.3 does not validate and escape the "order" and "orderby" GET parameters before using them in a SQL statement when viewing logs, leading to SQL injections issues	7.2	More Details
CVE-2021-24662	The Game Server Status WordPress plugin through 1.0 does not validate or escape the server_id parameter before using it in SQL statement, leading to an Authenticated SQL Injection in an admin page	7.2	More Details
CVE-2021-40345	An issue was discovered in Nagios XI 5.8.5. In the Manage Dashlets section of the Admin panel, an administrator can upload ZIP files. A command injection (within the name of the first file in the archive) allows an attacker to execute system commands.	7.2	More Details
CVE-2021-40344	An issue was discovered in Nagios XI 5.8.5. In the Custom Includes section of the Admin panel, an administrator can upload files with arbitrary extensions as long as the MIME type corresponds to an image. Therefore it is possible to upload a crafted PHP script to achieve remote command execution.	7.2	More Details
CVE-2021-42716	An issue was discovered in stb stb_image.h 2.27. The PNM loader incorrectly interpreted 16-bit PGM files as 8-bit when converting to RGBA, leading to a buffer overflow when later reinterpreting the result as a 16-bit buffer. An attacker could potentially have crashed a service using stb_image, or read up to 1024 bytes of non-consecutive heap data without control over the read location.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-23060	Internet Download Manager 6.37.11.1 was discovered to contain a stack buffer overflow in the Export/Import function. This vulnerability allows attackers to escalate local process privileges via a crafted ef2 file.	7.1	More Details
CVE-2021-35610	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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 as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H).	7.1	More Details
CVE-2021-35619	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 19c and 21c. Difficult to exploit vulnerability allows low privileged attacker having Create Procedure 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 takeover of Java VM. CVSS 3.1 Base Score 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H).	7.1	More Details
CVE-2021-0703	In SecondStageMain of init.cpp, there is a possible use after free due to incorrect shared_ptr usage. This could lead to local escalation of privilege if the attacker has physical access to the device, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-184569329	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35567	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via Kerberos to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Oracle GraalVM 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 Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:N/A:N).	6.8	More Details
CVE-2021-21319	Galette is a membership management web application geared towards non profit organizations. In versions prior to 0.9.5, malicious javascript code can be stored to be displayed later on self subscription page. The self subscription feature can be disabled as a workaround (this is the default state). Malicious javascript code can be executed (not stored) on login and retrieve password pages. This issue is patched in version 0.9.5.	6.8	More Details
CVE-2021-2414	Vulnerability in the Oracle Communications Session Border Controller product of Oracle Communications (component: Routing). Supported versions that are affected are 8.4 and 9.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Communications Session Border Controller. While the vulnerability is in Oracle Communications Session Border Controller, 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 Communications Session Border Controller accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.8	More Details
CVE-2021-35231	As a result of an unquoted service path vulnerability present in the Kiwi Syslog Server Installation Wizard, a local attacker could gain escalated privileges by inserting an executable into the path of the affected service or uninstall entry. Example vulnerable path: "Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Kiwi Syslog Server\Parameters\Application".	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35230	As a result of an unquoted service path vulnerability present in the Kiwi CatTools Installation Wizard, a local attacker could gain escalated privileges by inserting an executable into the path of the affected service or uninstall entry.	6.7	More Details
CVE-2021-42327	dp_link_settings_write in drivers/gpu/drm/amd/display/amdgpu_dm/amdgpu_dm_debugfs.c in the Linux kernel through 5.14.14 allows a heap-based buffer overflow by an attacker who can write a string to the AMD GPU display drivers debug filesystem. There are no checks on size within parse_write_buffer_into_params when it uses the size of copy_from_user to copy a userspace buffer into a 40-byte heap buffer.	6.7	More Details
CVE-2020-28964	Internet Download Manager 6.37.11.1 was discovered to contain a stack buffer overflow in the Search function. This vulnerability allows attackers to escalate local process privileges via unspecified vectors.	6.7	More Details
CVE-2021-0935	In ip6_xmit of ip6_output.c, there is a possible out of bounds write due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-168607263References: Upstream kernel	6.7	More Details
CVE-2021-0634	In display driver, there is a possible memory corruption due to uninitialized data. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594994; Issue ID: ALPS05594994.	6.7	More Details
CVE-2021-0941	In bpf_skb_change_head of filter.c, there is a possible out of bounds read due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-154177719References: Upstream kernel	6.7	More Details
CVE-2021-2332	Vulnerability in the Oracle LogMiner component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Easily exploitable vulnerability allows high privileged attacker having DBA privilege with network access via Oracle Net to compromise Oracle LogMiner. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle LogMiner accessible data as well as unauthorized read access to a subset of Oracle LogMiner accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle LogMiner. CVSS 3.1 Base Score 6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:H).	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0940	In TBD of TBD, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege in the kernel with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-171315276References: N/A	6.7	More Details
CVE-2021-0663	In audio DSP, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05844458; Issue ID: ALPS05844458.	6.7	More Details
CVE-2021-0662	In audio DSP, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05844434; Issue ID: ALPS05844434.	6.7	More Details
CVE-2021-0661	In audio DSP, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05844413; Issue ID: ALPS05844413.	6.7	More Details
CVE-2021-0633	In display driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05585423; Issue ID: ALPS05585423.	6.7	More Details
CVE-2021-0625	In ccu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594996; Issue ID: ALPS05594996.	6.7	More Details
CVE-2021-42739	The firewire subsystem in the Linux kernel through 5.14.13 has a buffer overflow related to drivers/media/firewire/firedtv-avc.c and drivers/media/firewire/firedtv-ci.c, because avc_ca_pmt mishandles bounds checking.	6.7	More Details
CVE-2021-23877	Privilege escalation vulnerability in the Windows trial installer of McAfee Total Protection (MTP) prior to 16.0.34_x may allow a local user to run arbitrary code as the admin user by replacing a specific temporary file created during the installation of the trial version of MTP.	6.7	More Details
CVE-2021-1966	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35545	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.28. 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 and unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.7 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:H).	6.7	More Details
CVE-2021-41179	Nextcloud is an open-source, self-hosted productivity platform. Prior to Nextcloud Server versions 20.0.13, 21.0.5, and 22.2.0, the Two-Factor Authentication wasn't enforced for pages marked as public. Any page marked as `@PublicPage` could thus be accessed with a valid user session that isn't authenticated. This particularly affects the Nextcloud Talk application, as this could be leveraged to gain access to any private chat channel without going through the Two-Factor flow. It is recommended that the Nextcloud Server be upgraded to 20.0.13, 21.0.5 or 22.2.0. There are no known workarounds aside from upgrading.	6.5	More Details
CVE-2021-2481	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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-2021-38479	Many API function codes receive raw pointers remotely from the user and trust these pointers as valid in-bound memory regions. An attacker can manipulate API functions by writing arbitrary data into the resolved address of a raw pointer.	6.5	More Details
CVE-2021-41182	jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `altField` option of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `altField` option is now treated as a CSS selector. A workaround is to not accept the value of the `altField` option from untrusted sources.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35539	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Filesystem). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, 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 Solaris. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).	6.5	More Details
CVE-2021-41135	The Cosmos-SDK is a framework for building blockchain applications in Golang. Affected versions of the SDK were vulnerable to a consensus halt due to non-deterministic behaviour in a ValidateBasic method in the x/authz module. The MsgGrant of the x/authz module contains a Grant field which includes a user-defined expiration time for when the authorization grant expires. In Grant.ValidateBasic(), that time is compared to the node's local clock time. Any chain running an affected version of the SDK with the authz module enabled could be halted by anyone with the ability to send transactions on that chain. Recovery would require applying the patch and rolling back the latest block. Users are advised to update to version 0.44.2.	6.5	More Details
CVE-2021-35582	Vulnerability in the Oracle Applications Manager product of Oracle E-Business Suite (component: View Reports). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Manager accessible data as well as unauthorized read access to a subset of Oracle Applications Manager accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Applications Manager. CVSS 3.1 Base Score 6.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L).	6.5	More Details
CVE-2021-41308	Affected versions of Atlassian Jira Server and Data Center allow authenticated yet non-administrator remote attackers to edit the File Replication settings via a Broken Access Control vulnerability in the `ReplicationSettings!default.jspa` endpoint. The affected versions are before version 8.6.0, from version 8.7.0 before 8.13.12, and from version 8.14.0 before 8.20.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35597	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 8.0.26 and prior. Easily exploitable 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 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-2021-35512	An SSRF issue was discovered in Zoho ManageEngine Applications Manager build 15200.	6.5	More Details
CVE-2021-41183	jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of various `*Text` options of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. The values passed to various `*Text` options are now always treated as pure text, not HTML. A workaround is to not accept the value of the `*Text` options from untrusted sources.	6.5	More Details
CVE-2021-41184	jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `of` option of the `.position()` util from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `of` option is now treated as a CSS selector. A workaround is to not accept the value of the `of` option from untrusted sources.	6.5	More Details
CVE-2021-41168	Snudown is a reddit-specific fork of the Sundown Markdown parser used by GitHub, with Python integration added. In affected versions snudown was found to be vulnerable to denial of service attacks to its reference table implementation. References written in markdown ` [reference_name]: https://www.example.com` are inserted into a hash table which was found to have a weak hash function, meaning that an attacker can reliably generate a large number of collisions for it. This makes the hash table vulnerable to a hash-collision DoS attack, a type of algorithmic complexity attack. Further the hash table allowed for duplicate entries resulting in long retrieval times. Proofs of concept and further discussion of the hash collision issue are discussed on the snudown GHSA(https://github.com/reddit/snudown/security/advisories/GHSA-6gvv-9q92-w5f6). Users are advised to update to version 1.7.0.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35607	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 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-2021-35609	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: SQR). Supported versions that are affected are 8.57, 8.58 and 8.59. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools 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-2020-36488	An issue in the FTP server of Sky File v2.1.0 allows attackers to perform directory traversal via `/null//` path commands.	6.5	More Details
CVE-2021-34860	This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of D-Link DAP-2020 1.01rc001 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the getpage parameter provided to the webproc endpoint. 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 root. Was ZDI-CAN-12103.	6.5	More Details
CVE-2021-34855	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 16.1.3 (49160). An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13592.	6.5	More Details
CVE-2021-24779	The WP Debugging WordPress plugin before 2.11.0 has its update_settings() function hooked to admin_init and is missing any authorisation and CSRF checks, as a result, the settings can be updated by unauthenticated users.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39126	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to modify various resources via a Cross-Site Request Forgery (CSRF) vulnerability, following an Information Disclosure vulnerability in the referrer headers which discloses a user's CSRF token. The affected versions are before version 8.5.10, and from version 8.6.0 before 8.13.1.	6.5	More Details
CVE-2021-0632	In wifi driver, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure to a proximal attacker under certain build conditions with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05560246; Issue ID: ALPS05551383.	6.5	More Details
CVE-2021-34596	A crafted request may cause a read access to an uninitialized pointer in CODESYS V2 Runtime Toolkit 32 Bit full and PLCWinNT prior to versions V2.4.7.56, resulting in a denial-of-service condition.	6.5	More Details
CVE-2021-41172	AS_Redis is an AntSword plugin for Redis. The Redis Manage plugin for AntSword prior to version 0.5 is vulnerable to Self-XSS due to due to insufficient input validation and sanitization via redis server configuration. Self-XSS in the plugin configuration leads to code execution. This issue is patched in version 0.5.	6.4	More Details
CVE-2021-39221	Nextcloud is an open-source, self-hosted productivity platform. The Nextcloud Contacts application prior to version 4.0.3 was vulnerable to a stored Cross-Site Scripting (XSS) vulnerability. For exploitation, a user would need to right-click on a malicious file and open the file in a new tab. Due the strict Content-Security-Policy shipped with Nextcloud, this issue is not exploitable on modern browsers supporting Content-Security-Policy. It is recommended that the Nextcloud Contacts application is upgraded to 4.0.3. As a workaround, one may use a browser that has support for Content-Security-Policy.	6.4	More Details
CVE-2021-35621	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35592	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	6.3	More Details
CVE-2021-35598	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	6.3	More Details
CVE-2021-42534	The affected product’s web application does not properly neutralize the input during webpage generation, which could allow an attacker to inject code in the input forms.	6.3	More Details
CVE-2021-35594	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35593	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	6.3	More Details
CVE-2021-35590	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	6.3	More Details
CVE-2021-1969	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	6.2	More Details
CVE-2021-1968	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	6.2	More Details
CVE-2021-41169	Sulu is an open-source PHP content management system based on the Symfony framework. In versions before 1.6.43 are subject to stored cross site scripting attacks. HTML input into Tag names is not properly sanitized. Only admin users are allowed to create tags. Users are advised to upgrade.	6.2	More Details
CVE-2020-23054	A cross-site scripting (XSS) vulnerability in NSK User Agent String Switcher Service v0.3.5 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the user agent input field.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29835	IBM Business Automation Workflow 18.0, 19.0, 20.0, and 21.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204833.	6.1	More Details
CVE-2020-23051	Phpgurukul User Registration & User Management System v2.0 was discovered to contain multiple stored cross-site scripting (XSS) vulnerabilities via the firstname and lastname parameters of the registration form & loginsystem input fields.	6.1	More Details
CVE-2021-31682	The login portal for the Automated Logic WebCTRL/WebCTRL OEM web application contains a vulnerability that allows for reflected XSS attacks due to the operatorlocale GET parameter not being sanitized. This issue impacts versions 6.5 and below. This issue works by passing in a basic XSS payload to a vulnerable GET parameter that is reflected in the output without sanitization.	6.1	More Details
CVE-2020-23042	Dropouts Technologies LLP Super Backup v2.0.5 was discovered to contain a cross-site scripting (XSS) vulnerability in the path parameter of the `list` and `download` module. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted GET request.	6.1	More Details
CVE-2020-23048	SeedDMS Content Management System v6.0.7 contains a persistent cross-site scripting (XSS) vulnerability in the component AddEvent.php via the name and comment parameters.	6.1	More Details
CVE-2020-23046	DedeCMS v7.5 SP2 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the component tpl.php via the `filename`, `mid`, `userid`, and `templet' parameters.	6.1	More Details
CVE-2020-23047	Macrob7 Macs Framework Content Management System - 1.14f was discovered to contain a cross-site scripting (XSS) vulnerability in the search input field of the search module.	6.1	More Details
CVE-2021-41747	Cross-Site Scripting (XSS) vulnerability exists in Csdn APP 4.10.0, which can be exploited by attackers to obtain sensitive information such as user cookies.	6.1	More Details
CVE-2020-23041	Dropouts Technologies LLP Air Share v1.2 was discovered to contain a cross-site scripting (XSS) vulnerability in the path parameter of the `list` and `download` exception-handling. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted GET request.	6.1	More Details
CVE-2020-36486	Swift File Transfer Mobile v1.1.2 and below was discovered to contain a cross-site scripting (XSS) vulnerability via the 'path' parameter of the 'list' and 'download' exception-handling.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34738	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) Software could allow an attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. For more information about these vulnerabilities, see the Details section of this advisory.	6.1	More Details
CVE-2020-22864	A cross site scripting (XSS) vulnerability in the Insert Video function of Froala WYSIWYG Editor 3.1.0 allows attackers to execute arbitrary web scripts or HTML.	6.1	More Details
CVE-2021-35568	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Rich Text Editor). Supported versions that are affected are 8.57, 8.58 and 8.59. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks 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-2021-35580	Vulnerability in the Oracle Applications Manager product of Oracle E-Business Suite (component: View Reports). 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 Applications Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Manager accessible data as well as unauthorized read access to a subset of Oracle Applications Manager accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41304	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability in the /secure/admin/ImporterFinishedPage.jspa error message. The affected versions are before version 8.13.12, and from version 8.14.0 before 8.20.2.	6.1	More Details
CVE-2021-35595	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Business Interlink). Supported versions that are affected are 8.57, 8.58 and 8.59. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks 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-2021-24885	The YOP Poll WordPress plugin before 6.1.2 does not escape the perpage parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2021-24543	The jQuery Reply to Comment WordPress plugin through 1.31 does not have any CSRF check when saving its settings, nor sanitise or escape its 'Quote String' and 'Reply String' settings before outputting them in Comments, leading to a Stored Cross-Site Scripting issue.	6.1	More Details
CVE-2021-35665	Vulnerability in the Hyperion Financial Reporting product of Oracle Hyperion (component: Repository). The supported version that is affected is 11.2.6.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Hyperion Financial Reporting. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Hyperion Financial Reporting, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Hyperion Financial Reporting accessible data as well as unauthorized read access to a subset of Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25969	In Camaleon CMS application, versions 0.0.1 to 2.6.0 are vulnerable to stored XSS, that allows an unauthenticated attacker to store malicious scripts in the comments section of the post. These scripts are executed in a victim's browser when they open the page containing the malicious comment.	6.1	More Details
CVE-2021-21747	ZTE MF971R product has reflective XSS vulnerability. An attacker could use the vulnerability to obtain cookie information.	6.1	More Details
CVE-2021-38896	IBM QRadar Advisor 2.5 through 2.6.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 209566.	6.1	More Details
CVE-2021-21746	ZTE MF971R product has reflective XSS vulnerability. An attacker could use the vulnerability to obtain cookie information.	6.1	More Details
CVE-2020-36502	Swift File Transfer Mobile v1.1.2 was discovered to contain a cross-site scripting (XSS) vulnerability via the devicename parameter which allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered as the device name itself.	6.1	More Details
CVE-2020-36495	DedeCMS v7.5 SP2 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the component file_manage_view.php via the `filename`, `mid`, `userid`, and `templet' parameters.	6.1	More Details
CVE-2021-28975	WP Mailster 1.6.18.0 allows XSS when a victim opens a mail server's details in the mst_servers page, for a crafted server_host, server_name, or connection_parameter parameter.	6.1	More Details
CVE-2020-36496	DedeCMS v7.5 SP2 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the component sys_admin_user_edit.php via the `filename`, `mid`, `userid`, and `templet' parameters.	6.1	More Details
CVE-2021-40121	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) Software could allow an attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. For more information about these vulnerabilities, see the Details section of this advisory.	6.1	More Details
CVE-2020-36497	DedeCMS v7.5 SP2 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the component makehtml_homepage.php via the `filename`, `mid`, `userid`, and `templet' parameters.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36494	DedeCMS v7.5 SP2 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the component mychannel_edit.php via the `filename`, `mid`, `userid`, and `templet' parameters.	6.1	More Details
CVE-2021-35589	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Device drivers). The supported version that is affected is 11. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, 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 Solaris. 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-2021-41171	eLabFTW is an open source electronic lab notebook manager for research teams. In versions of eLabFTW before 4.1.0, it allows attackers to bypass a brute-force protection mechanism by using many different forged PHPSESSID values in HTTP Cookie header. This issue has been addressed by implementing brute force login protection, as recommended by Owasp with Device Cookies. This mechanism will not impact users and will effectively thwart any brute-force attempts at guessing passwords. The only correct way to address this is to upgrade to version 4.1.0. Adding rate limitation upstream of the eLabFTW service is of course a valid option, with or without upgrading.	5.9	More Details
CVE-2021-2471	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Connectors accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Connectors. CVSS 3.1 Base Score 5.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:H).	5.9	More Details
CVE-2020-23036	MEDIA NAVI Inc SMACom v1.2 was discovered to contain an insecure session validation vulnerability in the session handling of the `password` authentication parameter of the wifi photo transfer module. This vulnerability allows attackers with network access privileges or on public wifi networks to read the authentication credentials and follow-up requests containing the user password via a man in the middle attack.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35666	Vulnerability in the Oracle HTTP Server product of Oracle Fusion Middleware (component: OSSL Module). The supported version that is affected is 11.1.1.9.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle HTTP Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle HTTP Server accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	5.9	More Details
CVE-2021-40122	A vulnerability in an API of the Call Bridge feature of Cisco Meeting Server could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. This vulnerability is due to improper handling of large series of message requests. An attacker could exploit this vulnerability by sending a series of messages to the vulnerable API. A successful exploit could allow the attacker to cause the affected device to reload, dropping all ongoing calls and resulting in a DoS condition.	5.9	More Details
CVE-2021-35550	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41158	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.10.7, an attacker can perform a SIP digest leak attack against FreeSWITCH and receive the challenge response of a gateway configured on the FreeSWITCH server. This is done by challenging FreeSWITCH's SIP requests with the realm set to that of the gateway, thus forcing FreeSWITCH to respond with the challenge response which is based on the password of that targeted gateway. Abuse of this vulnerability allows attackers to potentially recover gateway passwords by performing a fast offline password cracking attack on the challenge response. The attacker does not require special network privileges, such as the ability to sniff the FreeSWITCH's network traffic, to exploit this issue. Instead, what is required for this attack to work is the ability to cause the victim server to send SIP request messages to the malicious party. Additionally, to exploit this issue, the attacker needs to specify the correct realm which might in some cases be considered secret. However, because many gateways are actually public, this information can easily be retrieved. The vulnerability appears to be due to the code which handles challenges in `sofia_reg.c`, `sofia_reg_handle_sip_r_challenge()` which does not check if the challenge is originating from the actual gateway. The lack of these checks allows arbitrary UACs (and gateways) to challenge any request sent by FreeSWITCH with the realm of the gateway being targeted. This issue is patched in version 10.10.7. Maintainers recommend that one should create an association between a SIP session for each gateway and its realm to make a check be put into place for this association when responding to challenges.	5.8	More Details
CVE-2021-41159	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP), released under the Apache license. All FreeRDP clients prior to version 2.4.1 using gateway connections (`/gt:rpc`) fail to validate input data. A malicious gateway might allow client memory to be written out of bounds. This issue has been resolved in version 2.4.1. If you are unable to update then use `/gt:http` rather than /gt:rdp connections if possible or use a direct connection without a gateway.	5.8	More Details
CVE-2021-41188	Shopware is open source e-commerce software. Versions prior to 5.7.6 contain a cross-site scripting vulnerability. This issue is patched in version 5.7.6. Two workarounds are available. Using the security plugin or adding a particular following config to the `.htaccess` file will protect against cross-site scripting in this case. There is also a config for those using nginx as a server. The plugin and the configs can be found on the GitHub Security Advisory page for this vulnerability.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41173	Go Ethereum is the official Golang implementation of the Ethereum protocol. Prior to version 1.10.9, a vulnerable node is susceptible to crash when processing a maliciously crafted message from a peer. Version v1.10.9 contains patches to the vulnerability. There are no known workarounds aside from upgrading.	5.7	More Details
CVE-2021-28496	On systems running Arista EOS and CloudEOS with the affected release version, when using shared secret profiles the password configured for use by BiDirectional Forwarding Detection (BFD) will be leaked when displaying output over eAPI or other JSON outputs to other authenticated users on the device. The affected EOS Versions are: all releases in 4.22.x train, 4.23.9 and below releases in the 4.23.x train, 4.24.7 and below releases in the 4.24.x train, 4.25.4 and below releases in the 4.25.x train, 4.26.1 and below releases in the 4.26.x train	5.7	More Details
CVE-2021-35606	Vulnerability in the PeopleSoft Enterprise CS Campus Community product of Oracle PeopleSoft (component: Notification Framework). Supported versions that are affected are 9.0 and 9.2. Easily exploitable vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the PeopleSoft Enterprise CS Campus Community executes to compromise PeopleSoft Enterprise CS Campus Community. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise CS Campus Community accessible data. CVSS 3.1 Base Score 5.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	5.7	More Details
CVE-2021-35601	Vulnerability in the PeopleSoft Enterprise CS SA Integration Pack product of Oracle PeopleSoft (component: Students Administration). Supported versions that are affected are 9.0 and 9.2. Easily exploitable vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the PeopleSoft Enterprise CS SA Integration Pack executes to compromise PeopleSoft Enterprise CS SA Integration Pack. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise CS SA Integration Pack accessible data. CVSS 3.1 Base Score 5.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	5.7	More Details
CVE-2021-42299	Microsoft Surface Pro 3 Security Feature Bypass Vulnerability	5.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0411	In flv extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561362; Issue ID: ALPS05561362.	5.5	More Details
CVE-2021-0412	In flv extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561366; Issue ID: ALPS05561366.	5.5	More Details
CVE-2021-0618	In ape extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561394; Issue ID: ALPS05561394.	5.5	More Details
CVE-2021-0617	In ape extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561391; Issue ID: ALPS05561391.	5.5	More Details
CVE-2021-0616	In ape extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561389; Issue ID: ALPS05561389.	5.5	More Details
CVE-2021-0409	In flv extractor, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561359; Issue ID: ALPS05561359.	5.5	More Details
CVE-2021-0615	In flv extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561369; Issue ID: ALPS05561369.	5.5	More Details
CVE-2021-0614	In asf extractor, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05495528; Issue ID: ALPS05495528.	5.5	More Details
CVE-2021-0613	In asf extractor, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05489178.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0410	In flv extractor, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561360; Issue ID: ALPS05561360.	5.5	More Details
CVE-2021-0414	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561384; Issue ID: ALPS05561384.	5.5	More Details
CVE-2021-0413	In flv extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561379; Issue ID: ALPS05561379.	5.5	More Details
CVE-2021-0938	In memzero_explicit of compiler-clang.h, there is a possible bypass of defense in depth due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-171418586References: Upstream kernel	5.5	More Details
CVE-2021-35228	This vulnerability occurred due to missing input sanitization for one of the output fields that is extracted from headers on specific section of page causing a reflective cross site scripting attack. An attacker would need to perform a Man in the Middle attack in order to change header for a remote victim.	5.5	More Details
CVE-2021-39356	The Content Staging WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and escaping via several parameters that are echo'd out via the ~/templates/settings.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 2.0.1. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.	5.5	More Details
CVE-2021-0706	In startListening of PluginManagerImpl.java, there is a possible way to disable arbitrary app components due to a missing permission check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-193444889	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35540	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.28. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	5.5	More Details
CVE-2021-0702	In RevertActiveSessions of apexd.cpp, there is a possible way to share the wrong file due to an unintentional MediaStore downgrade. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-193932765	5.5	More Details
CVE-2021-0651	In loadLabel of PackageItemInfo.java, there is a possible way to DoS a device by having a long label in an app due to incorrect input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-9 Android-10Android ID: A-67013844	5.5	More Details
CVE-2021-0643	In getAllSubInfoList of SubscriptionController.java, there is a possible way to retrieve a long term identifier without the correct permissions due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12Android ID: A-183612370	5.5	More Details
CVE-2021-42556	Rasa X before 0.42.4 allows Directory Traversal during archive extraction. In the functionality that allows a user to load a trained model archive, an attacker has arbitrary write capability within specific directories via a crafted archive file.	5.5	More Details
CVE-2021-35551	Vulnerability in the RDBMS Security component of Oracle Database Server. Supported versions that are affected are 12.2.0.1, 19c and 21c. Easily exploitable vulnerability allows high privileged attacker having DBA privilege with network access via Oracle Net to compromise RDBMS Security. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of RDBMS Security as well as unauthorized update, insert or delete access to some of RDBMS Security accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39357	The Leaky Paywall WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via the ~/class.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 4.16.5. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.	5.5	More Details
CVE-2021-42715	An issue was discovered in stb stb_image.h 1.33 through 2.27. The HDR loader parsed truncated end-of-file RLE scanlines as an infinite sequence of zero-length runs. An attacker could potentially have caused denial of service in applications using stb_image by submitting crafted HDR files.	5.5	More Details
CVE-2021-35604	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.35 and prior and 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	5.5	More Details
CVE-2021-35612	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	5.5	More Details
CVE-2021-39328	The Simple Job Board WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient escaping on the $job_board_privacy_policy_label variable echo'd out via the ~/admin/settings/class-simple-job-board-settings-privacy.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 2.9.4. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39348	The LearnPress WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient escaping on the $custom_profile parameter found in the ~/inc/admin/views/backend-user-profile.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 4.1.3.1. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled. Please note that this is seperate from CVE-2021-24702.	5.5	More Details
CVE-2021-41791	An issue was discovered in Hyland org.alfresco:share through 7.0.0.2 and org.alfresco:community-share through 7.0. An evasion of the XSS filter for HTML input validation in the Alfresco Share User Interface leads to stored XSS that could be exploited by an attacker (given that he has privileges on the content collaboration features).	5.4	More Details
CVE-2021-25977	In PiranhaCMS, versions 7.0.0 to 9.1.1 are vulnerable to stored XSS due to the page title improperly sanitized. By creating a page with a specially crafted page title, a low privileged user can trigger arbitrary JavaScript execution.	5.4	More Details
CVE-2020-23039	Folder Lock v3.4.5 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the Create Folder function under the 'create' module. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload as a path or folder name.	5.4	More Details
CVE-2020-36499	TAO Open Source Assessment Platform v3.3.0 RC02 was discovered to contain a cross-site scripting (XSS) vulnerability in the content parameter of the Rubric Block (Add) module. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the rubric name value.	5.4	More Details
CVE-2020-36498	Macrob7 Macs Framework Content Management System - 1.14f contains a cross-site scripting (XSS) vulnerability in the account reset function, which allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the e-mail input field.	5.4	More Details
CVE-2020-36501	Multiple cross-site scripting (XSS) vulnerabilities in the Support module of SugarCRM v6.5.18 allows attackers to execute arbitrary web scripts or HTML via crafted payloads entered into the primary address state or alternate address state input fields.	5.4	More Details
CVE-2021-24699	The Easy Media Download WordPress plugin before 1.1.7 does not escape the text argument of its shortcode, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35649	Vulnerability in the Oracle Secure Global Desktop product of Oracle Virtualization (component: Server). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle Secure Global Desktop. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Secure Global Desktop accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Secure Global Desktop. CVSS 3.1 Base Score 5.4 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L).	5.4	More Details
CVE-2021-24414	The Video Player for YouTube WordPress plugin before 1.4 does not sanitise or validate the parameters from its shortcode, allowing users with a role as low as contributor to set Cross-Site Scripting payload in them which will be triggered in the page/s with the embed malicious shortcode	5.4	More Details
CVE-2021-24544	The Responsive WordPress Slider WordPress plugin through 2.2.0 does not sanitise and escape some of the Slider options, allowing Cross-Site Scripting payloads to be set in them. Furthermore, as by default any authenticated user is allowed to create Sliders (https://wordpress.org/support/topic/slider-can-be-changed-from-any-user-even-subscriber/, such settings can be changed in the plugin's settings), this would allow user with a role as low as subscriber to perform Cross-Site Scripting attacks against logged in admins viewing the slider list and could lead to privilege escalation by creating a rogue admin account for example.	5.4	More Details
CVE-2020-36492	DedeCMS v7.5 SP2 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the component select_media.php via the `activepath`, `keyword`, `tag`, `fmdo=x&filename`, `CKEditor` and `CKEditorFuncNum` parameters.	5.4	More Details
CVE-2020-20908	Akaunting v1.3.17 was discovered to contain a stored cross-site scripting (XSS) vulnerability which allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the Company Name input field.	5.4	More Details
CVE-2021-35616	Vulnerability in the Oracle Transportation Management product of Oracle Supply Chain (component: UI Infrastructure). The supported version that is affected is 6.4.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Transportation Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Transportation Management accessible data as well as unauthorized read access to a subset of Oracle Transportation Management accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35571	Vulnerability in the PeopleSoft Enterprise CS Academic Advisement product of Oracle PeopleSoft (component: Advising Notes). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise CS Academic Advisement. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise CS Academic Advisement accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise CS Academic Advisement accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	5.4	More Details
CVE-2020-5669	Cross-site scripting vulnerability in Movable Type Movable Type Premium 1.37 and earlier and Movable Type Premium Advanced 1.37 and earlier allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors.	5.4	More Details
CVE-2021-35553	Vulnerability in the PeopleSoft Enterprise CS Student Records product of Oracle PeopleSoft (component: Class Search). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise CS Student Records. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise CS Student Records, 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 CS Student Records accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise CS Student Records 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-2021-35541	Vulnerability in the PeopleSoft Enterprise SCM product of Oracle PeopleSoft (component: Supplier Portal). 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 SCM. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise SCM, 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 SCM accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise SCM accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36493	DedeCMS v7.5 SP2 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the component media_main.php via the `activepath`, `keyword`, `tag`, `fmdo=x&filename`, `CKEditor` and `CKEditorFuncNum` parameters.	5.4	More Details
CVE-2021-41866	MyBB before 1.8.28 allows stored XSS because the displayed Template Name value in the Admin CP's theme management is not escaped properly.	5.4	More Details
CVE-2020-36491	DedeCMS v7.5 SP2 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the component tags_main.php via the `activepath`, `keyword`, `tag`, `fmdo=x&filename`, `CKEditor` and `CKEditorFuncNum` parameters.	5.4	More Details
CVE-2020-23044	DedeCMS v7.5 SP2 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the component file_pic_view.php via the `activepath`, `keyword`, `tag`, `fmdo=x&filename`, `CKEditor` and `CKEditorFuncNum` parameters.	5.4	More Details
CVE-2021-27746	"HCL Connections Security Update for Reflected Cross-Site Scripting (XSS) Vulnerability"	5.4	More Details
CVE-2020-28955	SugarCRM v6.5.18 was discovered to contain a cross-site scripting (XSS) vulnerability in the Create Employee module. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the First Name or Last Name input fields.	5.4	More Details
CVE-2020-28956	Multiple cross-site scripting (XSS) vulnerabilities in the Sales module of SugarCRM v6.5.18 allows attackers to execute arbitrary web scripts or HTML via crafted payloads entered into the primary address state or alternate address state input fields.	5.4	More Details
CVE-2020-28957	Multiple cross-site scripting (XSS) vulnerabilities in the Customer Add module of Foxlor v0.10.16 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the name, firstname, or username input fields.	5.4	More Details
CVE-2020-23055	ANCOM WLAN Controller (Wireless Series & Hotspot) WLC-1000 & WLC-4006 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the /authen/start/ module via the userid and password parameters.	5.4	More Details
CVE-2020-23052	Catalyst IT Ltd Mahara CMS v19.10.2 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the component groupfiles.php via the Number (Nombre) and Description (Descripción) parameters.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28961	Perfex CRM v2.4.4 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the component ./clients/client via the company name parameter.	5.4	More Details
CVE-2020-23049	Fork CMS Content Management System v5.8.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the `Displayname` field when using the `Add`, `Edit` or `Register' functions. This vulnerability allows attackers to execute arbitrary web scripts or HTML.	5.4	More Details
CVE-2021-31834	Stored Cross-Site Scripting vulnerability in McAfee ePolicy Orchestrator (ePO) prior to 5.10 Update 11 allows ePO administrators to inject arbitrary web script or HTML via multiple parameters where the administrator's entries were not correctly sanitized.	5.4	More Details
CVE-2020-36489	Dropouts Technologies LLP Air Share v1.2 was discovered to contain a cross-site scripting (XSS) vulnerability in the devicename parameter. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the devicename information.	5.4	More Details
CVE-2020-36490	DedeCMS v7.5 SP2 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the component file_manage_view.php via the `activepath`, `keyword`, `tag`, `fmdo=x&filename`, `CKEditor` and `CKEditorFuncNum` parameters.	5.4	More Details
CVE-2020-28968	Draytek VigorAP 1000C contains a stored cross-site scripting (XSS) vulnerability in the RADIUS Setting - RADIUS Server Configuration module. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the username input field.	5.4	More Details
CVE-2021-35556	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35608	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. 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-2021-35586	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	5.3	More Details
CVE-2021-35578	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	5.3	More Details
CVE-2021-41160	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP), released under the Apache license. In affected versions a malicious server might trigger out of bound writes in a connected client. Connections using GDI or SurfaceCommands to send graphics updates to the client might send `0` width/height or out of bound rectangles to trigger out of bound writes. With `0` width or heigth the memory allocation will be `0` but the missing bounds checks allow writing to the pointer at this (not allocated) region. This issue has been patched in FreeRDP 2.4.1.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35565	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	5.3	More Details
CVE-2021-35564	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Keytool). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).	5.3	More Details
CVE-2021-41792	An issue was discovered in Hyland org.alfresco:alfresco-content-services through 6.2.2.18 and org.alfresco:alfresco-transform-services through 1.3. A crafted HTML file, once uploaded, could trigger an unexpected request by the transformation engine. The response to the request is not available to the attacker, i.e., this is blind SSRF.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35561	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Utility). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	5.3	More Details
CVE-2021-35655	Vulnerability in the Essbase Administration Services product of Oracle Essbase (component: EAS Console). The supported versions that are affected are Prior to 11.1.2.4.046 and Prior to 21.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Essbase Administration Services. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Essbase Administration Services 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-2021-35559	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-2477	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Session Management). 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 Applications Framework. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Applications Framework. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	5.3	More Details
CVE-2021-35554	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: Quotes). 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 Trade Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Trade Management 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-2021-35552	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Diagnostics). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).	5.3	More Details
CVE-2021-42762	BubblewrapLauncher.cpp in WebKitGTK and WPE WebKit before 2.34.1 allows a limited sandbox bypass that allows a sandboxed process to trick host processes into thinking the sandboxed process is not confined by the sandbox, by abusing VFS syscalls that manipulate its filesystem namespace. The impact is limited to host services that create UNIX sockets that WebKit mounts inside its sandbox, and the sandboxed process remains otherwise confined. NOTE: this is similar to CVE-2021-41133.	5.3	More Details
CVE-2021-34736	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart. The vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41157	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. By default, SIP requests of the type SUBSCRIBE are not authenticated in the affected versions of FreeSWITCH. Abuse of this security issue allows attackers to subscribe to user agent event notifications without the need to authenticate. This abuse poses privacy concerns and might lead to social engineering or similar attacks. For example, attackers may be able to monitor the status of target SIP extensions. Although this issue was fixed in version v1.10.6, installations upgraded to the fixed version of FreeSWITCH from an older version, may still be vulnerable if the configuration is not updated accordingly. Software upgrades do not update the configuration by default. SIP SUBSCRIBE messages should be authenticated by default so that FreeSWITCH administrators do not need to explicitly set the `auth-subscriptions` parameter. When following such a recommendation, a new parameter can be introduced to explicitly disable authentication.	5.3	More Details
CVE-2021-39127	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to the query component JQL endpoint via a Broken Access Control vulnerability (BAC) vulnerability. The affected versions are before version 8.5.10, and from version 8.6.0 before 8.13.1.	5.3	More Details
CVE-2021-2476	Vulnerability in the Oracle Transportation Management product of Oracle Supply Chain (component: Authentication). The supported version that is affected is 6.4.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Transportation Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Transportation Management 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-2017-20007	Ingeteam INGEPAC DA AU AUC_1.13.0.28 (and before) web application allows access to a certain path that contains sensitive information that could be used by an attacker to execute more sophisticated attacks. An unauthenticated remote attacker with access to the device´s web service could exploit this vulnerability in order to obtain different configuration files.	5.3	More Details
CVE-2021-1967	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35225	Each authenticated Orion Platform user in a MSP (Managed Service Provider) environment can view and browse all NetPath Services from all that MSP's customers. This can lead to any user having a limited insight into other customer's infrastructure and potential data cross-contamination.	5.0	More Details
CVE-2021-35602	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.26 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-2021-2416	Vulnerability in the Oracle Communications Session Border Controller product of Oracle Communications (component: Routing). Supported versions that are affected are 8.4 and 9.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Communications Session Border Controller. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Communications Session Border Controller. 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-2021-35626	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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-2021-35624	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 5.7.35 and prior and 8.0.26 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 creation, deletion or modification access to critical data or all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35622	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.26 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-2021-35627	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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-2021-35629	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2021-35628	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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-2021-35569	Vulnerability in the Oracle Applications Manager product of Oracle E-Business Suite (component: Diagnostics). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Applications Manager accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35596	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Error Handling). Supported versions that are affected are 8.0.26 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-2021-35591	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 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-2021-35577	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via MySQL Protcol 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-2021-35575	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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-2021-2478	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 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-2021-35634	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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-2021-35546	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.26 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-2021-35537	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2021-2479	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 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-2021-35631	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: GIS). Supported versions that are affected are 8.0.26 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-2021-35630	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.26 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 creation, deletion or modification access to critical data or all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N).	4.9	More Details
CVE-2021-35635	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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-2021-35638	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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-2021-35641	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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-2021-35637	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.26 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-2021-35636	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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-2021-35647	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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-2021-35646	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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-2021-35645	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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-2021-35648	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 8.0.26 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-2021-25972	In Camaleon CMS, versions 2.1.2.0 to 2.6.0, are vulnerable to Server-Side Request Forgery (SSRF) in the media upload feature, which allows admin users to fetch media files from external URLs but fails to validate URLs referencing to localhost or other internal servers. This allows attackers to read files stored in the internal server.	4.9	More Details
CVE-2021-35644	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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-2021-35643	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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-2021-35642	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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-2021-35639	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.26 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-2021-36869	Reflected Cross-Site Scripting (XSS) vulnerability in WordPress Ivory Search plugin (versions <= 4.6.6). Vulnerable parameter: &post.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39223	Nextcloud is an open-source, self-hosted productivity platform. The Nextcloud Richdocuments application prior to versions 3.8.6 and 4.2.3 returned verbatim exception messages to the user. This could result in a full path disclosure on shared files. (e.g. an attacker could see that the file `shared.txt` is located within `/files/$username/Myfolder/Mysubfolder/shared.txt`). It is recommended that the Richdocuments application is upgraded to 3.8.6 or 4.2.3. As a workaround, disable the Richdocuments application in the app settings.	4.8	More Details
CVE-2021-24485	The Special Text Boxes WordPress plugin before 5.9.110 does not sanitise or escape some of its settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed.	4.8	More Details
CVE-2021-24381	The Ninja Forms Contact Form WordPress plugin before 3.5.8.2 does not sanitise and escape the custom class name of the form field created, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-31835	Cross-Site Scripting vulnerability in McAfee ePolicy Orchestrator (ePO) prior to 5.10 Update 11 allows ePO administrators to inject arbitrary web script or HTML via a specific parameter where the administrator's entries were not correctly sanitized.	4.8	More Details
CVE-2021-34760	A vulnerability in the web-based management interface of Cisco TelePresence Management Suite (TMS) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by inserting malicious data in a specific data field in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	4.8	More Details
CVE-2021-38451	The affected product's proprietary protocol CSC allows for calling numerous function codes. In order to call those function codes, the user must supply parameters. There is no sanitation on the value of the offset, which allows the client to specify any offset and read out-of-bounds data.	4.8	More Details
CVE-2021-24489	The Request a Quote WordPress plugin before 2.3.9 does not sanitise, validate or escape some of its settings in the admin dashboard, leading to authenticated Stored Cross-Site Scripting issues even when the unfiltered_html capability is disallowed.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24514	The Visual Form Builder WordPress plugin before 3.0.4 does not sanitise or escape its Form Name, allowing high privilege users such as admin to set Cross-Site Scripting payload in them, even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2021-24515	The Video Gallery WordPress plugin before 1.1.5 does not escape the Title and Description of the videos in a gallery before outputting them in attributes, leading to Stored Cross-Site Scripting issues	4.8	More Details
CVE-2021-24608	The Formidable Form Builder – Contact Form, Survey & Quiz Forms Plugin for WordPress plugin before 5.0.07 does not sanitise and escape its Form's Labels, allowing high privileged users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2021-34789	A vulnerability in the web-based management interface of Cisco Tetration could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack on an affected system. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker would need valid administrative credentials.	4.8	More Details
CVE-2021-24785	The Great Quotes WordPress plugin through 1.0.0 does not sanitise and escape the Quote and Author fields of its Quotes, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed.	4.8	More Details
CVE-2021-24653	The Cookie Bar WordPress plugin before 1.8.9 doesn't properly sanitise the Cookie Bar Message setting, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2021-39354	The Easy Digital Downloads WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the $start_date and $end_date parameters found in the ~/includes/admin/payments/class-payments-table.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.11.2.	4.8	More Details
CVE-2021-40526	Incorrect calculation of buffer size vulnerability in Peleton TTR01 up to and including PTV55G allows a remote attacker to trigger a Denial of Service attack through the GymKit daemon process by exploiting a heap overflow in the network server handling the Apple GymKit communication. This can lead to an Apple MFI device not being able to authenticate with the Peleton Bike	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24744	The WordPress Contact Forms by Cimatti WordPress plugin before 1.4.12 does not sanitise and escape the Form Title before outputting it in some admin pages. which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed.	4.8	More Details
CVE-2021-35581	Vulnerability in the Oracle Applications Manager product of Oracle E-Business Suite (component: View Reports). 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 Applications Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Manager 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-2021-35227	The HTTP interface was enabled for RabbitMQ Plugin in ARM 2020.2.6 and the ability to configure HTTPS was not available.	4.7	More Details
CVE-2021-35650	Vulnerability in the Oracle Secure Global Desktop product of Oracle Virtualization (component: Client). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle Secure Global Desktop. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Secure Global Desktop accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Secure Global Desktop. CVSS 3.1 Base Score 4.6 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:L).	4.6	More Details
CVE-2020-23058	An issue in the authentication mechanism in Nong Ge File Explorer v1.4 unauthenticated allows to access sensitive data.	4.6	More Details
CVE-2021-0939	In set_default_passthru_cfg of passthru.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-186026549References: N/A	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35632	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Data Dictionary). Supported versions that are affected are 8.0.26 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-2021-35542	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.28. 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-2021-2475	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.28. 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-2021-35558	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 19c and 21c. Easily exploitable vulnerability allows low privileged attacker having Create Table privilege with network access via Oracle Net to compromise Core RDBMS. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Core RDBMS. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34743	A vulnerability in the application integration feature of Cisco Webex Software could allow an unauthenticated, remote attacker to authorize an external application to integrate with and access a user's account without that user's express consent. This vulnerability is due to improper validation of cross-site request forgery (CSRF) tokens. An attacker could exploit this vulnerability by convincing a targeted user who is currently authenticated to Cisco Webex Software to follow a link designed to pass malicious input to the Cisco Webex Software application authorization interface. A successful exploit could allow the attacker to cause Cisco Webex Software to authorize an application on the user's behalf without the express consent of the user, possibly allowing external applications to read data from that user's profile.	4.3	More Details
CVE-2021-42096	GNU Mailman before 2.1.35 may allow remote Privilege Escalation. A certain csrf_token value is derived from the admin password, and may be useful in conducting a brute-force attack against that password.	4.3	More Details
CVE-2021-21745	ZTE MF971R product has a Referer authentication bypass vulnerability. Without CSRF verification, an attackercould use this vulnerability to perform illegal authorization operations by sending a request to the user to click.	4.3	More Details
CVE-2021-35584	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: ndbcluster/plugin DDL). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Cluster. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 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-2021-21743	ZTE MF971R product has a CRLF injection vulnerability. An attacker could exploit the vulnerability to modify the HTTP response header information through a specially crafted HTTP request.	4.3	More Details
CVE-2021-35557	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 19c and 21c. Easily exploitable vulnerability allows low privileged attacker having Create Table privilege with network access via Oracle Net to compromise Core RDBMS. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Core RDBMS. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	4.3	More Details
CVE-2021-25971	In Camaleon CMS, versions 2.0.1 to 2.6.0 are vulnerable to an Uncaught Exception. The app's media upload feature crashes permanently when an attacker with a low privileged access uploads a specially crafted .svg file	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40123	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker with administrative read-only privileges to download files that should be restricted. This vulnerability is due to incorrect permissions settings on an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request to the device. A successful exploit could allow the attacker to download files that should be restricted.	4.3	More Details
CVE-2021-41176	Pterodactyl is an open-source game server management panel built with PHP 7, React, and Go. In affected versions of Pterodactyl a malicious user can trigger a user logout if a signed in user visits a malicious website that makes a request to the Panel's sign-out endpoint. This requires a targeted attack against a specific Panel instance, and serves only to sign a user out. **No user details are leaked, nor is any user data affected, this is simply an annoyance at worst.** This is fixed in version 1.6.3.	4.3	More Details
CVE-2021-35611	Vulnerability in the Oracle Sales Offline product of Oracle E-Business Suite (component: Offline Template). 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 Sales Offline. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Sales Offline. 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-2021-29883	IBM Standards Processing Engine (IBM Transformation Extender Advanced 9.0 and 10.0) 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: 207090.	4.3	More Details
CVE-2020-14263	"HCL Traveler Companion is vulnerable to an iOS weak cryptographic process vulnerability via the included MobileIron AppConnect SDK"	3.9	More Details
CVE-2021-35549	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Utility). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.1 Base Score 3.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L).	3.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14264	"HCL Traveler Companion is vulnerable to an iOS weak cryptographic process vulnerability via the included MobileIron AppConnect SDK"	3.9	More Details
CVE-2021-35603	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (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-2021-35613	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Cluster. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	3.7	More Details
CVE-2021-2480	Vulnerability in the Oracle HTTP Server product of Oracle Fusion Middleware (component: Web Listener). The supported version that is affected is 11.1.1.9.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HTTP Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle HTTP Server accessible data. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	3.7	More Details
CVE-2021-39220	Nextcloud is an open-source, self-hosted productivity platform The Nextcloud Mail application prior to versions 1.10.4 and 1.11.0 does by default not render images in emails to not leak the read state or user IP. The privacy filter failed to filter images with a relative protocol. It is recommended that the Nextcloud Mail application is upgraded to 1.10.4 or 1.11.0. There are no known workarounds aside from upgrading.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39224	Nextcloud is an open-source, self-hosted productivity platform. The Nextcloud OfficeOnline application prior to version 1.1.1 returned verbatim exception messages to the user. This could result in a full path disclosure on shared files. (e.g. an attacker could see that the file `shared.txt` is located within `/files/$username/Myfolder/Mysubfolder/shared.txt`). It is recommended that the OfficeOnline application is upgraded to 1.1.1. As a workaround, one may disable the OfficeOnline application in the app settings.	3.5	More Details
CVE-2021-35588	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 7u311, 8u301; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L).	3.1	More Details
CVE-2021-35625	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.26 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-2021-35623	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.26 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 Number	Description	Base Score	Reference
CVE-2021-35576	Vulnerability in the Oracle Database Enterprise Edition Unified Audit component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Easily exploitable vulnerability allows high privileged attacker having Local Logon privilege with network access via Oracle Net to compromise Oracle Database Enterprise Edition Unified Audit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Database Enterprise Edition Unified Audit accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).	2.7	More Details
CVE-2021-35640	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).	2.7	More Details
CVE-2021-35633	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Logging). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).	2.7	More Details
CVE-2021-35618	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 1.8 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:N/I:N/A:L).	1.8	More Details
CVE-2020-7859	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3542	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-42739. Reason: This candidate is a reservation duplicate of CVE-2021-42739. Notes: All CVE users should reference CVE-2021-42739 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-40719	Adobe Connect version 11.2.3 (and earlier) is affected by a Deserialization of Untrusted Data vulnerability to achieve arbitrary method invocation when AMF messages are deserialized on an Adobe Connect server. An attacker can leverage this to execute remote code execution on the server.	N/A	More Details