Vulnerability Summary for the Week of April 19, 2021

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by Ug-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of Ug-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- robohelp	Adobe Robohelp version 2020.0.3 (and earlier) is affected by an uncontrolled search path element vulnerability that could lead to privilege escalation. An attacker with permissions to write to the file system could leverage this vulnerability to escalate privileges.	2021-04-19	9.3	CVE-2021-21070 MISC
autodesk -- fbx_review	A user may be tricked into opening a malicious FBX file which may exploit a Directory Traversal Remote Code Execution vulnerability in FBX's Review causing it to run arbitrary code on the system.	2021-04-19	9.3	CVE-2021-27030 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
autodesk -- fbx_review	A user may be tricked into opening a malicious FBX file which may exploit a use-after-free vulnerability in FBX's Review causing the application to reference a memory location controlled by an unauthorized third party, thereby running arbitrary code on the system.	2021-04-19	9.3	CVE-2021-27031 MISC MISC
canonical -- ubuntu_linux	The overlayfs implementation in the linux kernel did not properly validate with respect to user namespaces the setting of file capabilities on files in an underlying file system. Due to the combination of unprivileged user namespaces along with a patch carried in the Ubuntu kernel to allow unprivileged overlay mounts, an attacker could use this to gain elevated privileges.	2021-04-17	7.2	CVE-2021-3493 MISC MISC MISC
canonical -- ubuntu_linux	Shiftfs, an out-of-tree stacking file system included in Ubuntu Linux kernels, did not properly handle faults occurring during copy_from_user() correctly. These could lead to either a double-free situation or memory not being freed at all. An attacker could use this to cause a denial of service (kernel memory exhaustion) or gain privileges via executing arbitrary code. AKA ZDI-CAN-13562.	2021-04-17	7.2	CVE-2021-3492 MISC MISC MISC MISC MISC
cnesty -- helpcom	A vulnerability of Helpcom could allow an unauthenticated attacker to execute arbitrary command.	2021-04-20	7.5	CVE-2020-7856 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	This vulnerability exists due to insufficient authentication validation.			
ffmpegdotjs_project -- ffmpegdotjs	This affects all versions of package ffmpegdotjs. If attacker-controlled user input is given to the trimvideo function, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization.	2021-04-18	7.5	CVE-2021-23376 MISC MISC
fibaro -- home_center_2_firmware	In Fibaro Home Center 2 and Lite devices with firmware version 4.540 and older an authenticated user can run commands as root user using a command injection vulnerability.	2021-04-19	9	CVE-2021-20991 CONFIRM FULLDISC MISC
fibaro -- home_center_2_firmware	In Fibaro Home Center 2 and Lite devices with firmware version 4.600 and older an internal management service is accessible on port 8000 and some API endpoints could be accessed without authentication to trigger a shutdown, a reboot or a reboot into recovery mode.	2021-04-19	7.8	CVE-2021-20990 CONFIRM FULLDISC MISC
killing_project -- killing	This affects all versions of package killing. If attacker-controlled user input is given, it is possible for an attacker to execute arbitrary commands. This is due to	2021-04-18	7.5	CVE-2021-23381

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	use of the child_process exec function without input sanitization.			MISC MISC
lextudio -- restructuredtext	vscode-restructuredtext before 146.0.0 contains an incorrect access control vulnerability, where a crafted project folder could execute arbitrary binaries via crafted workspace configuration.	2021-04-20	7.5	CVE-2021-28793 MISC MISC MISC MISC
onion-oled-js_project -- onion-oled-js	This affects all versions of package onion-oled-js. If attacker-controlled user input is given to the scroll function, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization.	2021-04-18	7.5	CVE-2021-23377 MISC MISC
openclinic_ga_project -- openclinic_ga	An exploitable SQL injection vulnerability exists in ‘getAssets.jsp’ page of OpenClinic GA 5.173.3. The componentStatus parameter in the getAssets.jsp page is vulnerable to unauthenticated SQL injection An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-04-19	7.5	CVE-2020-27240 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openclinic_ga_project -- openclinic_ga	An exploitable SQL injection vulnerability exists in 'getAssets.jsp' page of OpenClinic GA 5.173.3. The serialnumber parameter in the getAssets.jsp page is vulnerable to unauthenticated SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-04-19	7.5	CVE-2020-27241 MISC
oracle -- enterprise_manager	Vulnerability in the Enterprise Manager for Fusion Middleware product of Oracle Enterprise Manager (component: FMW Control Plugin). The supported version that is affected are 11.1.1.9 and 12.2.1.3 Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Enterprise Manager for Fusion Middleware. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Enterprise Manager for Fusion Middleware accessible data as well as unauthorized read access to a subset of Enterprise Manager for Fusion Middleware accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Enterprise Manager for Fusion Middleware. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	2021-04-22	7.5	CVE-2021-2008 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- secure_global_desktop	Vulnerability in the Oracle Secure Global Desktop product of Oracle Virtualization (component: Gateway). The supported version that is affected is 5.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Secure Global Desktop. While the vulnerability is in Oracle Secure Global Desktop, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Secure Global Desktop. CVSS 3.1 Base Score 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).	2021-04-22	7.5	CVE-2021-2177 MISC
oracle -- weblogic_server	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 T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2021-04-22	7.5	CVE-2021-2135 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. 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).	2021-04-22	7.5	CVE-2021-2136 MISC
picotts_project -- picotts	This affects all versions of package picotts. If attacker-controlled user input is given to the say function, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization.	2021-04-18	7.5	CVE-2021-23378 MISC MISC
portkiller_project -- portkiller	This affects all versions of package portkiller. If (attacker-controlled) user input is given, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization.	2021-04-18	7.5	CVE-2021-23379 MISC MISC
ps-visitor_project -- ps-visitor	This affects all versions of package ps-visitor. If attacker-controlled user input is given to the kill	2021-04-18	7.5	CVE-2021-23374

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	function, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization.			MISC MISC
psnode_project -- psnode	This affects all versions of package psnode. If attacker-controlled user input is given to the kill function, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization.	2021-04-18	7.5	CVE-2021-23375 MISC MISC
qnap -- qts	An SQL injection vulnerability has been reported to affect QNAP NAS running Multimedia Console or the Media Streaming add-on. If exploited, the vulnerability allows remote attackers to obtain application information. QNAP has already fixed this vulnerability in the following versions of Multimedia Console and the Media Streaming add-on. QTS 4.3.3: Media Streaming add-on 430.1.8.10 and later QTS 4.3.6: Media Streaming add-on 430.1.8.8 and later QTS 4.4.x and later: Multimedia Console 1.3.4 and later We have also fixed this vulnerability in the following versions of QTS 4.3.3 and QTS 4.3.6, respectively: QTS 4.3.3.1624 Build 20210416 or later QTS 4.3.6.1620 Build 20210322 or later	2021-04-17	7.5	CVE-2020-36195 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qnap -- qts	A command injection vulnerability has been reported to affect QTS and QuTS hero. If exploited, this vulnerability allows attackers to execute arbitrary commands in a compromised application. We have already fixed this vulnerability in the following versions: QTS 4.5.2.1566 Build 20210202 and later QTS 4.5.1.1495 Build 20201123 and later QTS 4.3.6.1620 Build 20210322 and later QTS 4.3.4.1632 Build 20210324 and later QTS 4.3.3.1624 Build 20210416 and later QTS 4.2.6 Build 20210327 and later QuTS hero h4.5.1.1491 build 20201119 and later	2021-04-17	7.5	CVE-2020-2509 MISC
roar-pidusage_project -- roar-pidusage	This affects all versions of package roar-pidusage. If attacker-controlled user input is given to the stat function of this package on certain operating systems, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization.	2021-04-18	7.5	CVE-2021-23380 MISC MISC
rpm_spec_project -- rpm_spec	The unofficial vscode-rpm-spec extension before 0.3.2 for Visual Studio Code allows remote code execution via a crafted workspace configuration.	2021-04-16	7.5	CVE-2021-31414 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tendacn -- g0_firmware	Command Injection in Tenda G0 routers with firmware versions v15.11.0.6(9039)_CN and v15.11.0.5(5876)_CN , and Tenda G1 and G3 routers with firmware versions v15.11.0.17(9502)_CN or v15.11.0.16(9024)_CN allows remote attackers to execute arbitrary OS commands via a crafted action/setDebugCfg request. This occurs because the "formSetDebugCfg" function executes glibc's system function with untrusted input.	2021-04-16	10	CVE-2021-27691 MISC
tendacn -- g1_firmware	Command Injection in Tenda G1 and G3 routers with firmware versions v15.11.0.17(9502)_CN or v15.11.0.16(9024)_CN allows remote attackers to execute arbitrary OS commands via a crafted "action/umountUSBPartition" request. This occurs because the "formSetUSBPartitionUmount" function executes the "doSystemCmd" function with untrusted input.	2021-04-16	10	CVE-2021-27692 MISC
wondercms -- wondercms	A remote code execution vulnerability in the installUpdateThemePluginAction function in index.php in WonderCMS 3.1.3, allows remote attackers to upload a custom plugin which can contain arbitrary code and obtain a webshell via the theme/plugin installer.	2021-04-20	7.5	CVE-2020-35314 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wondercms -- wondercms	A server-side request forgery (SSRF) vulnerability in the addCustomThemePluginRepository function in index.php in WonderCMS 3.1.3 allows remote attackers to execute arbitrary code via a crafted URL to the theme/plugin installer.	2021-04-20	7.5	CVE-2020-35313 MISC MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- genuine_service	Adobe Genuine Service version 6.6 (and earlier) is affected by an Uncontrolled Search Path element vulnerability. An authenticated attacker could exploit this to to plant custom binaries and execute them with System permissions. Exploitation of this issue requires user interaction.	2021-04-16	6.9	CVE-2020-9667 MISC
adtran -- personal_phone_manager	** UNSUPPORTED WHEN ASSIGNED ** The AdTran Personal Phone Manager	2021-04-20	4.3	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	software is vulnerable to multiple reflected cross-site scripting (XSS) issues. These issues impact at minimum versions 10.8.1 and below but potentially impact later versions as well since they have not previously been disclosed. Only version 10.8.1 was able to be confirmed during primary research. NOTE: The affected appliances NetVanta 7060 and NetVanta 7100 are considered End of Life and as such this issue will not be patched.			25680 MISC MISC MISC
adtran -- personal_phone_manager	** UNSUPPORTED WHEN ASSIGNED ** AdTran Personal Phone Manager 10.8.1 software is vulnerable to an issue that allows for exfiltration of data over DNS. This could allow for exposed AdTran Personal Phone Manager web servers to be used as DNS redirectors to tunnel arbitrary data over DNS. NOTE: The affected appliances NetVanta 7060 and NetVanta 7100 are considered End of Life and as such this issue will not be patched.	2021-04-20	5	CVE-2021-25681 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
alpinelinux -- apk-tools	In Alpine Linux apk-tools before 2.12.5, the tarball parser allows a buffer overflow and crash.	2021-04-21	5	CVE-2021-30139 MISC MISC
atlassian -- connect_express	Broken Authentication in Atlassian Connect Express (ACE) from version 3.0.2 before version 6.6.0: Atlassian Connect Express is a Node.js package for building Atlassian Connect apps. Authentication between Atlassian products and the Atlassian Connect Express app occurs with a server-to-server JWT or a context JWT. Atlassian Connect Express versions between 3.0.2 - 6.5.0 erroneously accept context JWTs in lifecycle endpoints (such as installation) where only server-to-server JWTs should be accepted, permitting an attacker to send authenticated re-installation events to an app.	2021-04-16	4	CVE-2021-26073 N/A MISC
atlassian -- connect_spring_boot	Broken Authentication in Atlassian Connect Spring Boot (ACSB) from version 1.1.0 before version 2.1.3: Atlassian	2021-04-16	4	CVE-2021-26074

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Connect Spring Boot is a Java Spring Boot package for building Atlassian Connect apps. Authentication between Atlassian products and the Atlassian Connect Spring Boot app occurs with a server-to-server JWT or a context JWT. Atlassian Connect Spring Boot versions between 1.1.0 - 2.1.2 erroneously accept context JWTs in lifecycle endpoints (such as installation) where only server-to-server JWTs should be accepted, permitting an attacker to send authenticated re-installation events to an app.			N/A N/A
autodesk -- fbx_review	A Out-Of-Bounds Read/Write Vulnerability in Autodesk FBX Review version 1.4.0 may lead to remote code execution through maliciously crafted DLL files or information disclosure.	2021-04-19	6.8	CVE-2021-27027 MISC MISC MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
autodesk -- fbx_review	A Memory Corruption Vulnerability in Autodesk FBX Review version 1.4.0 may lead to remote code execution through maliciously crafted DLL files.	2021-04-19	6.8	CVE-2021-27028 MISC MISC MISC
autodesk -- fbx_review	The user may be tricked into opening a malicious FBX file which may exploit a Null Pointer Dereference vulnerability in FBX's Review causing the application to crash leading to a denial of service.	2021-04-19	4.3	CVE-2021-27029 MISC MISC
curveballjs -- a12n-server	a12n-server is an npm package which aims to provide a simple authentication system. A new HAL-Form was added to allow editing users in version 0.18.0. This feature should only have been accessible to admins. Unfortunately, privileges were incorrectly checked allowing any logged in user to make this change. Patched in v0.18.2.	2021-04-16	4	CVE-2021-29452 MISC CONFIRM
ezxml_project -- ezxml	An issue was discovered in libezxml.a in ezXML 0.8.6. The function	2021-04-16	4.3	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ezxml_parse_str() performs incorrect memory handling while parsing crafted XML files (out-of-bounds read after a certain strcspn failure).			31348 MISC
ezxml_project -- ezxml	An issue was discovered in libezxml.a in ezXML 0.8.6. The function ezxml_parse_str() performs incorrect memory handling while parsing crafted XML files (writing outside a memory region created by mmap).	2021-04-16	4.3	CVE-2021-31347 MISC
fibaro -- home_center_2_firmware	Fibaro Home Center 2 and Lite devices with firmware version 4.600 and older initiate SSH connections to the Fibaro cloud to provide remote access and remote support capabilities. This connection can be intercepted using DNS spoofing attack and a device initiated remote port-forward channel can be used to connect to the web management interface. Knowledge of authorization credentials to the management interface is required to perform any further actions.	2021-04-19	4.3	CVE-2021-20989 CONFIRM FULLDISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fibaro -- home_center_2_firmware	In Fibaro Home Center 2 and Lite devices in all versions provide a web based management interface over unencrypted HTTP protocol. Communication between the user and the device can be eavesdropped to hijack sessions, tokens and passwords.	2021-04-19	5	CVE-2021-20992 CONFIRM FULLDISC MISC
google -- bazel	An attacker can place a crafted JSON config file into the project folder pointing to a custom executable. VScode-bazel allows the workspace path to lint *.bzl files to be set via this config file. As such the attacker is able to execute any executable on the system through vscode-bazel. We recommend upgrading to version 0.4.1 or above.	2021-04-16	6.8	CVE-2021-22539 MISC MISC
gpac -- gpac	There is a Null Pointer Dereference in function filter_core/filter_pck.c:gf_filter_pck_new_alloc_internal in GPAC 1.0.1. The pid comes from function av1dmx_parse_flush_sample,	2021-04-19	4.3	CVE-2021-30015 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the ctx.opid maybe NULL. The result is a crash in gf_filter_pck_new_alloc_internal.			
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 1.0.1. There is heap-based buffer overflow in the function gp_rtp_builder_do_avc() in ietf/rtp_pck_mpeg4.c.	2021-04-21	6.8	CVE-2020-35979 MISC MISC
gpac -- gpac	An issue was discovered in gpac before 1.0.1. A NULL pointer dereference exists in the function dump_isom_sdp located in filedump.c. It allows an attacker to cause Denial of Service.	2021-04-21	4.3	CVE-2020-23932 MISC MISC
gpac -- gpac	There is a integer overflow in media_tools/av_parsers.c in the hevc_parse_slice_segment function in GPAC 1.0.1 which results in a crash.	2021-04-19	4.3	CVE-2021-30014 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gpac -- gpac	Memory leak in the stbl_GetSampleInfos function in MP4Box in GPAC 1.0.1 allows attackers to read memory via a crafted file.	2021-04-19	4.3	CVE-2021-31256 MISC MISC
gpac -- gpac	In the adts_dmx_process function in filters/reframe_adts.c in GPAC 1.0.1, a crafted file may cause ctx->hdr.frame_size to be smaller than ctx->hdr.hdr_size, resulting in size to be a negative number and a heap overflow in the memcpy.	2021-04-19	4.3	CVE-2021-30019 MISC MISC
gpac -- gpac	In the function gf_hevc_read_pps_bs_internal function in media_tools/av_parsers.c in GPAC 1.0.1 there is a loop, which with crafted file, pps->num_tile_columns may be larger than sizeof(pps->column_width), which results in a heap overflow in the loop.	2021-04-19	4.3	CVE-2021-30020 MISC MISC
gpac -- gpac	There is a integer overflow in media_tools/av_parsers.c in the gf_avc_read_pps_bs_internal in GPAC	2021-04-19	4.3	CVE-2021-30022

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	1.0.1. pps_id may be a negative number, so it will not return. However, avc->pps only has 255 unit, so there is an overflow, which results a crash.			MISC MISC
gpac -- gpac	In filters/reframe_latm.c in GPAC 1.0.1 there is a Null Pointer Dereference, when gf_filter_pck_get_data is called. The first arg pck may be null with a crafted mp4 file,which results in a crash.	2021-04-19	4.3	CVE-2021-30199 MISC MISC
gpac -- gpac	The gf_isom_set_extraction_slc function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command.	2021-04-19	4.3	CVE-2021-31258 MISC MISC
gpac -- gpac	The gf_isom_cenc_get_default_info_internal function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command.	2021-04-19	4.3	CVE-2021-31259 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gpac -- gpac	The MergeTrack function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command.	2021-04-19	4.3	CVE-2021-31260 MISC MISC
gpac -- gpac	The gf_hinter_track_new function in GPAC 1.0.1 allows attackers to read memory via a crafted file in the MP4Box command.	2021-04-19	4.3	CVE-2021-31261 MISC MISC
gpac -- gpac	The AV1_DuplicateConfig function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command.	2021-04-19	4.3	CVE-2021-31262 MISC MISC
gpac -- gpac	The HintFile function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command.	2021-04-19	4.3	CVE-2021-31257 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gpac -- gpac	An issue was discovered in gpac through 20200801. A NULL pointer dereference exists in the function nhmldump_send_header located in write_nhml.c. It allows an attacker to cause Denial of Service.	2021-04-21	4.3	CVE-2020-23930 MISC MISC
gpac -- gpac	Buffer overflow in the tenc_box_read function in MP4Box in GPAC 1.0.1 allows attackers to cause a denial of service or execute arbitrary code via a crafted file, related invalid IV sizes.	2021-04-19	6.8	CVE-2021-31254 MISC MISC
gpac -- gpac	An issue was discovered in gpac before 1.0.1. The abst_box_read function in box_code_adobe.c has a heap-based buffer over-read.	2021-04-21	5.8	CVE-2020-23931 MISC MISC MISC
gpac -- gpac	Buffer overflow in the abst_box_read function in MP4Box in GPAC 1.0.1 allows attackers to cause a denial of service or execute arbitrary code via a crafted file.	2021-04-19	6.8	CVE-2021-31255

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 1.0.1. There is a use-after-free in the function gf_isom_box_del() in isomedia/box_funcs.c.	2021-04-21	6.8	CVE-2020-35980 MISC MISC
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 1.0.1. There is an invalid pointer dereference in the function SetupWriters() in isomedia/isom_store.c.	2021-04-21	6.8	CVE-2020-35981 MISC MISC
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 1.0.1. There is an invalid pointer dereference in the function gf_hinter_track_finalize() in media_tools/isom_hinter.c.	2021-04-21	6.8	CVE-2020-35982 MISC MISC
gpac -- gpac	An issue was discovered in gpac before 1.0.1. The abst_box_read function in	2021-04-21	5.8	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	box_code_adobe.c has a heap-based buffer over-read.			23928 MISC MISC MISC
gpac -- gpac	There is a integer overflow in function filter_core/filter_props.c:gf_props_assign_value in GPAC 1.0.1. In which, the arg const GF_PropertyValue *value,maybe value->value.data.size is a negative number. In result, memcpy in gf_props_assign_value failed.	2021-04-19	6.8	CVE-2021-29279 MISC MISC
hashicorp -- consul	HashiCorp Consul Enterprise version 1.8.0 up to 1.9.4 audit log can be bypassed by specifically crafted HTTP events. Fixed in 1.9.5, and 1.8.10.	2021-04-20	5	CVE-2021-28156 MISC MISC
hashicorp -- consul	HashiCorp Consul and Consul Enterprise up to version 1.9.4 key-value (KV) raw mode was vulnerable to cross-site scripting. Fixed in 1.9.5, 1.8.10 and 1.7.14.	2021-04-20	4.3	CVE-2020-25864 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- i	IBM i 7.1, 7.2, 7.3, and 7.4 SMTP allows a network attacker to send emails to non-existent local-domain recipients to the SMTP server, caused by using a non-default configuration. An attacker could exploit this vulnerability to consume unnecessary network bandwidth and disk space, and allow remote attackers to send spam email. IBM X-Force ID: 198056.	2021-04-21	6.4	CVE-2021-20501 XF CONFIRM
ibm -- resilient	IBM Resilient SOAR V38.0 could allow a privileged user to create create malicious scripts that could be executed as another user. IBM X-Force ID: 198759.	2021-04-19	6.5	CVE-2021-20527 CONFIRM XF
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 196649.	2021-04-21	6.4	CVE-2021-20454 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- websphere_application_server	IBM WebSphere Application Server 8.0, 8.5, and 9.0 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 196648.	2021-04-20	6.4	CVE-2021-20453 CONFIRM XF
innorix -- file_transfer_solution	Innorix Web-Based File Transfer Solution versuibs prior to and including 9.2.18.385 contains a vulnerability that could allow remote files to be downloaded and executed by setting the arguments to the internal method. A remote attacker could induce a user to access a crafted web page, causing damage such as malicious code infection.	2021-04-19	6.8	CVE-2020-7851 MISC MISC
jenkins -- config_file_provider	Jenkins Config File Provider Plugin 3.7.0 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	2021-04-21	5.5	CVE-2021-21642 CONFIRM MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jenkins -- config_file_provider	Jenkins Config File Provider Plugin 3.7.0 and earlier does not correctly perform permission checks in several HTTP endpoints, allowing attackers with global Job/Configure permission to enumerate system-scoped credentials IDs of credentials stored in Jenkins.	2021-04-21	4	CVE-2021-21643 CONFIRM MLIST
jose_project -- jose	jose-node-cjs-runtime is an npm package which provides a number of cryptographic functions. In versions prior to 3.11.4 the AES_CBC_HMAC_SHA2 Algorithm (A128CBC-HS256, A192CBC-HS384, A256CBC-HS512) decryption would always execute both HMAC tag verification and CBC decryption, if either failed `JWEDecryptionFailed` would be thrown. But a possibly observable difference in timing when padding error would occur while decrypting the ciphertext makes a padding oracle and an adversary might be able to make use of that oracle to decrypt data without knowing the decryption key by issuing on average 128*b calls to the padding oracle (where b is the number of	2021-04-16	4.3	CVE-2021-29446 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bytes in the ciphertext block). A patch was released which ensures the HMAC tag is verified before performing CBC decryption. The fixed versions are `>=3.11.4`. Users should upgrade to `^3.11.4`.			
jose_project -- jose	jose-node-esm-runtime is an npm package which provides a number of cryptographic functions. In versions prior to 3.11.4 the AES_CBC_HMAC_SHA2 Algorithm (A128CBC-HS256, A192CBC-HS384, A256CBC-HS512) decryption would always execute both HMAC tag verification and CBC decryption, if either failed `JWEDecryptionFailed` would be thrown. But a possibly observable difference in timing when padding error would occur while decrypting the ciphertext makes a padding oracle and an adversary might be able to make use of that oracle to decrypt data without knowing the decryption key by issuing on average 128*b calls to the padding oracle (where b is the number of bytes in the ciphertext block). A patch was released which ensures the HMAC tag is	2021-04-16	4.3	CVE-2021-29445 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	verified before performing CBC decryption. The fixed versions are `>=3.11.4`. Users should upgrade to `^3.11.4`.			
jose_project -- jose	jose is an npm library providing a number of cryptographic operations. In vulnerable versions AES_CBC_HMAC_SHA2 Algorithm (A128CBC-HS256, A192CBC-HS384, A256CBC-HS512) decryption would always execute both HMAC tag verification and CBC decryption, if either failed `JWEDecryptionFailed` would be thrown. A possibly observable difference in timing when padding error would occur while decrypting the ciphertext makes a padding oracle and an adversary might be able to make use of that oracle to decrypt data without knowing the decryption key by issuing on average 128*b calls to the padding oracle (where b is the number of bytes in the ciphertext block). All major release versions have had a patch released which ensures the HMAC tag is verified before performing CBC decryption. The fixed versions are `^1.28.1 || ^2.0.5 ||	2021-04-16	4.3	CVE-2021-29443 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	>=3.11.4`. Users should upgrade their v1.x dependency to ^1.28.1, their v2.x dependency to ^2.0.5, and their v3.x dependency to ^3.11.4. Thanks to Jason from Microsoft Vulnerability Research (MSVR) for bringing this up and Eva Sarafianou (@esarafianou) for helping to score this advisory.			
jose_project -- jose	jose-browser-runtime is an npm package which provides a number of cryptographic functions. In versions prior to 3.11.4 the AES_CBC_HMAC_SHA2 Algorithm (A128CBC-HS256, A192CBC-HS384, A256CBC-HS512) decryption would always execute both HMAC tag verification and CBC decryption, if either failed `JWEDecryptionFailed` would be thrown. But a possibly observable difference in timing when padding error would occur while decrypting the ciphertext makes a padding oracle and an adversary might be able to make use of that oracle to decrypt data without knowing the decryption key by issuing on average 128*b calls to the	2021-04-16	4.3	CVE-2021-29444 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	padding oracle (where b is the number of bytes in the ciphertext block). A patch was released which ensures the HMAC tag is verified before performing CBC decryption. The fixed versions are `>=3.11.4`. Users should upgrade to `^3.11.4`.			
manydesigns -- portofino	Portofino is an open source web development framework. Portofino before version 5.2.1 did not properly verify the signature of JSON Web Tokens. This allows forging a valid JWT. The issue will be patched in the upcoming 5.2.1 release.	2021-04-16	6.4	CVE-2021-29451 MISC CONFIRM MISC
mediawiki -- mediawiki	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. It improperly handled account blocks for certain automatically created MediaWiki user accounts, thus allowing nefarious users to remain unblocked.	2021-04-22	5.5	CVE-2021-31554 MISC MISC
mediawiki -- mediawiki	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. It	2021-04-22	5.5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	incorrectly executed certain rules related to blocking accounts after account creation. Such rules would allow for user accounts to be created while blocking only the IP address used to create an account (and not the user account itself). Such rules could also be used by a nefarious, unprivileged user to catalog and enumerate any number of IP addresses related to these account creations.			31552 MISC MISC
mediawiki -- mediawiki	An issue was discovered in the CheckUser extension for MediaWiki through 1.35.2. MediaWiki usernames with trailing whitespace could be stored in the cu_log database table such that denial of service occurred for certain CheckUser extension pages and functionality. For example, the attacker could turn off Special:CheckUserLog and thus interfere with usage tracking.	2021-04-22	6.4	CVE-2021-31553 MISC MISC MISC MISC MISC MISC MISC
mediawiki -- mediawiki	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. A MediaWiki user who is partially blocked or	2021-04-22	4	CVE-2021-31548

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	was unsuccessfully blocked could bypass AbuseFilter and have their edits completed.			MISC MISC
mediawiki -- mediawiki	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. Its AbuseFilterCheckMatch API reveals suppressed edits and usernames to unprivileged users through the iteration of crafted AbuseFilter rules.	2021-04-22	4	CVE-2021-31547 MISC MISC MISC
mediawiki -- mediawiki	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. It incorrectly logged sensitive suppression deletions, which should not have been visible to users with access to view AbuseFilter log data.	2021-04-22	4	CVE-2021-31546 MISC MISC
mediawiki -- mediawiki	An issue was discovered in the PageForms extension for MediaWiki through 1.35.2. Crafted payloads for Token-related query parameters allowed for XSS on certain PageForms-managed MediaWiki pages.	2021-04-22	4.3	CVE-2021-31551 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mediawiki -- mediawiki	An issue was discovered in the CommentBox extension for MediaWiki through 1.35.2. Via crafted configuration variables, a malicious actor could introduce XSS payloads into various layers.	2021-04-22	4.3	CVE-2021-31550 MISC MISC
mediawiki -- mediawiki	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. The Special:AbuseFilter/examine form allowed for the disclosure of suppressed MediaWiki usernames to unprivileged users.	2021-04-22	4	CVE-2021-31549 MISC MISC MISC
mediawiki -- mediawiki	An issue was discovered in the Oauth extension for MediaWiki through 1.35.2. It did not validate the oarc_version (aka oauth_registered_consumer.oarc_version) parameter's length.	2021-04-22	5	CVE-2021-31555 MISC MISC
mediawiki -- mediawiki	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. The page_recent_contributors leaked the existence of certain deleted MediaWiki usernames, related to rev_deleted.	2021-04-22	5	CVE-2021-31545 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mendix -- mendix	A vulnerability has been identified in Mendix Applications using Mendix 7 (All versions < V7.23.19), Mendix Applications using Mendix 8 (All versions < V8.17.0), Mendix Applications using Mendix 8 (V8.12) (All versions < V8.12.5), Mendix Applications using Mendix 8 (V8.6) (All versions < V8.6.9), Mendix Applications using Mendix 9 (All versions < V9.0.5). Authenticated, non-administrative users could modify their privileges by manipulating the user role under certain circumstances, allowing them to gain administrative privileges.	2021-04-16	6.5	CVE-2021-27394 CONFIRM
nvidia -- geforce_experience	NVIDIA GeForce Experience, all versions prior to 3.22, contains a vulnerability in GameStream plugins where log files are created using NT/System level permissions, which may lead to code execution, denial of service, or local privilege escalation.	2021-04-20	4.6	CVE-2021-1079 CONFIRM
omicronenergy -- stationguard	OMICRON StationGuard before 1.10 allows remote attackers to cause a denial of service (connectivity outage) via crafted	2021-04-20	5	CVE-2021-30464

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	tcp/20499 packets to the CTRL Ethernet port.			CONFIRM MISC
oracle -- applications_framework	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Home page). The supported version that is affected is 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 creation, deletion or modification access to critical data or all Oracle Applications Framework accessible data as well as unauthorized access to critical data or complete access to all Oracle Applications Framework accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	6.4	CVE-2021-2200 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- business_intelligence	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Actions). Supported versions that are affected are 5.5.0.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	2021-04-22	4.9	CVE-2021-2191 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- customers_online	Vulnerability in the Oracle Customers Online product of Oracle E-Business Suite (component: Customer Tab). 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 Customers Online. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Customers Online accessible data as well as unauthorized access to critical data or complete access to all Oracle Customers Online 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).	2021-04-22	5.5	CVE-2021-2156 MISC
oracle -- database_server	Vulnerability in the Recovery component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having DBA	2021-04-22	4	CVE-2021-2173 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Level Account privilege with network access via Oracle Net to compromise Recovery. While the vulnerability is in Recovery, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Recovery accessible data. CVSS 3.1 Base Score 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N).			
oracle -- database_server	Vulnerability in the Database Vault component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Any View, Select Any View privilege with network access via Oracle Net to compromise Database Vault. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Database Vault accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts).	2021-04-22	4	CVE-2021-2175 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).			
oracle -- document_management_and_collaboration	Vulnerability in the Oracle Document Management and Collaboration product of Oracle E-Business Suite (component: Attachments). 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 Document Management and Collaboration. While the vulnerability is in Oracle Document Management and Collaboration, 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 Document Management and Collaboration accessible data as well as unauthorized update, insert or delete access to some of Oracle Document Management and Collaboration accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and	2021-04-22	5.5	CVE-2021-2181 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:L/A:N).			
oracle -- email_center	Vulnerability in the Oracle Email Center product of Oracle E-Business Suite (component: Message Display). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Email Center. While the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.1 Base Score 8.5 (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).	2021-04-22	5.5	CVE-2021-2209 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- enterprise_manager	Vulnerability in the Enterprise Manager for Fusion Middleware product of Oracle Enterprise Manager (component: FMW Control Plugin). The supported version that is affected is 12.2.1.4. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Enterprise Manager for Fusion Middleware. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Enterprise Manager for Fusion Middleware. 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).	2021-04-22	4	CVE-2021-2134 MISC
oracle -- enterprise_manager_base_platform	Vulnerability in the Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: UI Framework). The supported version that is affected is 13.4.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise	2021-04-22	5.8	CVE-2021-2053 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Enterprise Manager Base Platform. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Enterprise Manager Base Platform, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Enterprise Manager Base Platform accessible data as well as unauthorized read access to a subset of Enterprise Manager Base Platform 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).			
oracle -- financial_services_analytical_applications_infrastructure	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Rules Framework). Supported versions that are affected are 8.0.6-8.1.0. Easily exploitable vulnerability allows unauthenticated	2021-04-22	5.8	CVE-2021-2140 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Analytical Applications Infrastructure, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Analytical Applications Infrastructure accessible data as well as unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure 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).			
oracle -- hyperion_financial_management	Vulnerability in the Hyperion Financial Management product of Oracle Hyperion (component: Task Automation). The	2021-04-22	4.6	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	supported version that is affected is 11.1.2.4. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Hyperion Financial Management. 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 Hyperion Financial Management accessible data as well as unauthorized read access to a subset of Hyperion Financial Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Hyperion Financial Management. CVSS 3.1 Base Score 3.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:L).			2158 MISC
oracle -- internet_expenses	Vulnerability in the Oracle Internet Expenses product of Oracle E-Business Suite (component: Mobile Expenses).	2021-04-22	4.3	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Supported versions that are affected are 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Internet Expenses. 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 Internet Expenses accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).			2153 MISC
oracle -- istore	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than	2021-04-22	5.8	CVE-2021-2183 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).			
oracle -- istore	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly	2021-04-22	5.8	CVE-2021-2182 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).			
oracle -- istore	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in	2021-04-22	5.8	CVE-2021-2150 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).			
oracle -- istore	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore	2021-04-22	5.8	CVE-2021-2199 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).			
oracle -- istore	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of	2021-04-22	5.8	CVE-2021-2184 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).			
oracle -- istore	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and	2021-04-22	5.8	CVE-2021-2185 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).			
oracle -- istore	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector:	2021-04-22	5.8	CVE-2021-2186 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).			
oracle -- istore	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2021-04-22	5.8	CVE-2021-2187 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- istore	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2021-04-22	5.8	CVE-2021-2188 MISC
oracle -- istore	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component:	2021-04-22	5.8	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).			2197 MISC
oracle -- knowledge_management	Vulnerability in the Oracle Knowledge Management product of Oracle E-Business Suite (component: Setup, Admin). Supported versions that are affected are	2021-04-22	5.8	CVE-2021-2198 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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 Knowledge Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Knowledge Management, 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 Knowledge Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Knowledge Management accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).			
oracle -- marketing	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration).	2021-04-22	6.4	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Supported versions that are affected are 12.2.7-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Marketing accessible data as well as unauthorized access to critical data or complete access to all Oracle Marketing accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).			2205 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this	2021-04-22	4	CVE-2021-2201 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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).			
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized 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).	2021-04-22	4	CVE-2021-2202 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2215 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized	2021-04-22	4	CVE-2021-2203 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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).			
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2208 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server:	2021-04-22	4	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).			2212 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of	2021-04-22	4	CVE-2021-2213 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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).			
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2196 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily	2021-04-22	4	CVE-2021-2230 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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).			
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector:	2021-04-22	4	CVE-2021-2217 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).			
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server 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).	2021-04-22	4	CVE-2021-2226 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via	2021-04-22	4	CVE-2021-2193 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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).			
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2278 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2293 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized	2021-04-22	4	CVE-2021-2298 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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).			
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2299 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server:	2021-04-22	4	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).			2300 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7	2021-04-22	4	CVE-2021-2301 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).			
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2305 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high	2021-04-22	4	CVE-2021-2308 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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).			
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2194 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized 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).	2021-04-22	4	CVE-2021-2178 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized	2021-04-22	4	CVE-2021-2180 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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).			
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 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).	2021-04-22	4	CVE-2021-2172 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are	2021-04-22	4	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).			2170 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score	2021-04-22	4	CVE-2021-2169 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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).			
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2164 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily	2021-04-22	4	CVE-2021-2179 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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).			
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of	2021-04-22	5.5	CVE-2021-2304 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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).			
oracle -- one-to-one_fulfillment	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Documents). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).	2021-04-22	4.3	CVE-2021-2155 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- partner_management	Vulnerability in the Oracle Partner Management product of Oracle E-Business Suite (component: Attribute Admin Setup). 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 Partner Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Partner Management, 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 Partner Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Partner Management accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2021-04-22	5.8	CVE-2021-2195 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- peoplesoft_enterprise	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Security). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of PeopleSoft Enterprise PeopleTools. 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).	2021-04-22	6.5	CVE-2021-2151 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Multichannel Framework). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2021-04-22	5.8	CVE-2021-2216 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- sales_offline	Vulnerability in the Oracle Sales Offline product of Oracle E-Business Suite (component: Template). 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 Sales Offline. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Sales Offline. 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).	2021-04-22	5	CVE-2021-2189 MISC
oracle -- sales_offline	Vulnerability in the Oracle Sales Offline product of Oracle E-Business Suite (component: Template). 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 Sales Offline.	2021-04-22	5	CVE-2021-2190 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Sales Offline. 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).			
oracle -- solaris	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Common Desktop Environment). The supported version that is affected is 10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in takeover of Oracle Solaris. 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).	2021-04-22	4.6	CVE-2021-2167 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- trade_management	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 require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, 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 Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2021-04-22	5.8	CVE-2021-2210 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- trade_management	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 require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, 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 Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2021-04-22	5.8	CVE-2021-2206 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	2021-04-22	4.4	CVE-2021-2145 MISC MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: TopLink Integration). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable	2021-04-22	5	CVE-2021-2157 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).			
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality	2021-04-22	5	CVE-2021-2204 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).			
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 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).	2021-04-22	4.3	CVE-2021-2211 MISC MISC
paloaltonetworks -- bridgecrew_checkov	An unsafe deserialization vulnerability in Bridgecrew Checkov by Prisma Cloud allows arbitrary code execution when	2021-04-20	6.5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	processing a malicious terraform file. This issue impacts Checkov 2.0 versions earlier than Checkov 2.0.26. Checkov 1.0 versions are not impacted.			3035 MISC
paloaltonetworks -- globalprotect	A denial-of-service (DoS) vulnerability in Palo Alto Networks GlobalProtect app on Windows systems allows a limited Windows user to send specifically-crafted input to the GlobalProtect app that results in a Windows blue screen of death (BSOD) error. This issue impacts: GlobalProtect app 5.1 versions earlier than GlobalProtect app 5.1.8; GlobalProtect app 5.2 versions earlier than GlobalProtect app 5.2.4.	2021-04-20	4.9	CVE-2021-3038 MISC
qnap -- quts_hero	A cross-site scripting (XSS) vulnerability has been reported to affect earlier versions of File Station. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions: QTS 4.5.2.1566 build 20210202 (and later) QTS 4.5.1.1456 build 20201015 (and later) QTS 4.3.6.1446 build 20200929	2021-04-16	4.3	CVE-2018-19942 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(and later) QTS 4.3.4.1463 build 20201006 (and later) QTS 4.3.3.1432 build 20201006 (and later) QTS 4.2.6 build 20210327 (and later) QuTS hero h4.5.1.1472 build 20201031 (and later) QuTScloud c4.5.4.1601 build 20210309 (and later) QuTScloud c4.5.3.1454 build 20201013 (and later)			
sonicwall -- email_security	SonicWall Email Security version 10.0.9.x contains a vulnerability that allows a post-authenticated attacker to read an arbitrary file on the remote host.	2021-04-20	4	CVE-2021-20023 CONFIRM
tibco -- administrator	The Administration GUI component of TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition for z/Linux, and TIBCO Administrator -	2021-04-20	6.5	CVE-2021-28828 CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Enterprise Edition for z/Linux contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute a SQL injection attack on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.10.2 and below, and TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.11.0 and 5.11.1.			
tibco -- administrator	The Administration GUI component of TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition	2021-04-20	6	CVE-2021-28829 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition for z/Linux, and TIBCO Administrator - Enterprise Edition for z/Linux contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute a persistent CSV injection attack from the affected 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 Administrator - Enterprise Edition: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.10.2 and below, and			CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.11.0 and 5.11.1.			
tribalsystems -- zenario	SQL Injection in Tribalsystems Zenario CMS 8.8.52729 allows remote attackers to access the database or delete the plugin. This is accomplished via the `ID` input field of ajax.php in the `Pugin library - delete` module.	2021-04-16	6.4	CVE-2021-26830 CONFIRM
vmware -- nsx-t_data_center	VMware NSX-T contains a privilege escalation vulnerability due to an issue with RBAC (Role based access control) role assignment. Successful exploitation of this issue may allow attackers with local guest user account to assign privileges higher than their own permission level.	2021-04-19	4.6	CVE-2021-21981 MISC
xmbforum2 -- xmb	XMB is vulnerable to cross-site scripting (XSS) due to inadequate filtering of BBCode input. This bug affects all versions of XMB. All XMB installations must be updated to versions 1.9.12.03 or 1.9.11.16.	2021-04-19	4.3	CVE-2021-29399 MISC MISC MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adtran -- personal_phone_manager	** UNSUPPORTED WHEN ASSIGNED ** The AdTran Personal Phone Manager software is vulnerable to an authenticated stored cross-site scripting (XSS) issues. These issues impact at minimum versions 10.8.1 and below but potentially impact later versions as well since they have not previously been disclosed. Only version 10.8.1 was able to be confirmed during primary research. NOTE: The affected appliances NetVanta 7060 and NetVanta 7100 are considered End of Life and as such this issue will not be patched.	2021-04-20	3.5	CVE-2021-25679 MISC MISC MISC MISC
ibm -- spectrum_protect	IBM Spectrum Protect Server 7.1 and 8.1 is subject to a stack-based buffer overflow caused by improper bounds checking during the parsing of commands. By issuing such a command with an improper parameter, an authorized administrator	2021-04-16	2.1	CVE-2021-20491 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	could overflow a buffer and cause the server to crash. IBM X-Force ID: 197792.			
linux -- linux_kernel	An issue was discovered in the Linux kernel through 5.11.x. kernel/bpf/verifier.c performs undesirable out-of-bounds speculation on pointer arithmetic, leading to side-channel attacks that defeat Spectre mitigations and obtain sensitive information from kernel memory. Specifically, for sequences of pointer arithmetic operations, the pointer modification performed by the first operation is not correctly accounted for when restricting subsequent operations.	2021-04-20	2.1	CVE-2021-29155 MISC MISC
mi -- miui	The application in the mobile phone can read the SNO information of the device, Xiaomi 10 MIUI < 2020.01.15.	2021-04-20	2.1	CVE-2020-14105 CONFIRM
online_discussion_forum_project -- online_discussion_forum	The messaging subsystem in the Online Discussion Forum 1.0 is vulnerable to	2021-04-19	3.5	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	XSS in the message body. An authenticated user can send messages to arbitrary users on the system that include javascript that will execute when viewing the messages page.			28141 EXPLOIT-DB
oracle -- business_intelligence	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web General). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business	2021-04-22	3.6	CVE-2021-2152 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 4.0 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:L/I:L/A:N).			
oracle -- database	Vulnerability in the Oracle Database - Enterprise Edition component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having RMAN executable privilege with logon to the infrastructure where Oracle Database - Enterprise Edition executes to compromise Oracle Database - Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Database - Enterprise Edition accessible data. CVSS 3.1 Base Score 2.3 (Integrity impacts). CVSS Vector:	2021-04-22	2.1	CVE-2021-2207 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).			
oracle -- flexcube_direct_banking	Vulnerability in the Oracle FLEXCUBE Direct Banking product of Oracle Financial Services Applications (component: Pre Login). Supported versions that are affected are 12.0.2 and 12.0.3. Difficult to exploit vulnerability allows high privileged attacker with network access via Oracle Net to compromise Oracle FLEXCUBE Direct Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Direct Banking accessible data. CVSS 3.1 Base Score 2.0 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:N).	2021-04-22	2.1	CVE-2021-2141 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.23 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 1.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L).	2021-04-22	1.9	CVE-2021-2232 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Packaging). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to	2021-04-22	3.3	CVE-2021-2307 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N).			
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.33 and prior and 8.0.23 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	2021-04-22	3.5	CVE-2021-2171 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).			
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	3.5	CVE-2021-2174 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- peoplesoft_enterprise_campus_software_campus_community	Vulnerability in the PeopleSoft Enterprise CS Campus Community product of Oracle PeopleSoft (component: Frameworks). 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 Campus Community. 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 PeopleSoft Enterprise CS Campus Community accessible data. CVSS 3.1 Base Score 3.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N).	2021-04-22	3.5	CVE-2021-2159 MISC
oracle -- solaris	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the	2021-04-22	3.6	CVE-2021-2192 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris as well as unauthorized update, insert or delete access to some of Oracle Solaris accessible data. Note: This vulnerability applies to Oracle Solaris on SPARC systems only. CVSS 3.1 Base Score 6.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H).			
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle	2021-04-22	3.5	CVE-2021-2214 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N).			
oracle -- zfs_storage_appliance	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Core). The supported version that is affected is 8.8. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle ZFS Storage Appliance Kit accessible data. CVSS 3.1 Base Score 2.5 (Integrity impacts). CVSS Vector:	2021-04-22	1.9	CVE-2021-2149 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N).			
oracle -- zfs_storage_appliance	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Installation). The supported version that is affected is 8.8. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle ZFS Storage Appliance Kit accessible data. CVSS 3.1 Base Score 1.8 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:N).	2021-04-22	1.2	CVE-2021-2147 MISC
paloaltonetworks -- pan-os	An information exposure through log file vulnerability exists in Palo Alto Networks	2021-04-20	2.1	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	PAN-OS software where secrets in PAN-OS XML API requests are logged in cleartext to the web server logs when the API is used incorrectly. This vulnerability applies only to PAN-OS appliances that are configured to use the PAN-OS XML API and exists only when a client includes a duplicate API parameter in API requests. Logged information includes the cleartext username, password, and API key of the administrator making the PAN-OS XML API request.			3036 MISC
paloaltonetworks -- pan-os	An information exposure through log file vulnerability exists in Palo Alto Networks PAN-OS software where the connection details for a scheduled configuration export are logged in system logs. Logged information includes the cleartext username, password, and IP address used to export the PAN-OS configuration to the destination server.	2021-04-20	2.1	CVE-2021-3037 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
remoteclinic -- remote_clinic	Cross Site Scripting (XSS) in Remote Clinic v2.0 via the "Chat" and "Personal Address" field on staff/register.php	2021-04-21	3.5	CVE-2021-31329 MISC
remoteclinic -- remote_clinic	Stored XSS in Remote Clinic v2.0 in /medicines due to Medicine Name Field.	2021-04-21	3.5	CVE-2021-31327 MISC
telegram -- telegram	The Telegram app 7.6.2 for iOS allows remote authenticated users to cause a denial of service (application crash) if the victim pastes an attacker-supplied message (e.g., in the Persian language) into a channel or group. The crash occurs in MtProtoKitFramework.	2021-04-20	3.5	CVE-2021-30496 MISC MISC