Vulnerability Summary for the Week of July 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
dlink -- dir-3040_firmware	A hard-coded password vulnerability exists in the Libcli Test Environment functionality of D-LINK DIR-3040 1.13B03. A specially crafted network request can lead to code execution. An attacker can send a sequence of requests to trigger this vulnerability.	2021-07-16	7.5	CVE-2021-21820 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- malware_protection_engine	Microsoft Defender Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34522.	2021-07-16	9.3	CVE-2021-34464 MISC
microsoft -- windows_10	Microsoft Windows Media Foundation Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34441, CVE-2021-34503.	2021-07-16	9.3	CVE-2021-34439 MISC
microsoft -- windows_10	Scripting Engine Memory Corruption Vulnerability	2021-07-16	9.3	CVE-2021-34448 MISC
microsoft -- windows_10	Windows Hyper-V Remote Code Execution Vulnerability	2021-07-16	9	CVE-2021-34450 MISC
microsoft -- windows_server_2016	Windows Kernel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34508.	2021-07-16	9	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				34458 MISC
oracle -- business_intelligence	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web General). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2021-07-21	7.5	CVE-2021-2456 MISC MISC
oracle -- commerce_platform	Vulnerability in the Oracle Commerce Platform product of Oracle Commerce (component: Dynamo Application Framework). Supported versions that are affected are 11.0.0, 11.1.0, 11.2.0 and 11.3.0-11.3.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Platform. Successful attacks of this vulnerability can result in takeover of Oracle Commerce Platform. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability	2021-07-21	7.5	CVE-2021-2463 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:H/I:H/A:H).			
oracle -- siebel_crm	Vulnerability in the Siebel CRM product of Oracle Siebel CRM (component: Siebel Core - Server Infrastructure). Supported versions that are affected are 21.5 and Prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Siebel CRM. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel CRM accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	2021-07-21	7.1	CVE-2021-2368 MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Security). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2021-07-21	7.5	CVE-2021-2382 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 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2021-07-21	7.5	CVE-2021-2397 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
advantech -- r-seenet	This vulnerability is present in device_graph_page.php script, which is a part of the Advantech R-SeeNet web applications.	2021-07-16	4.3	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	A specially crafted URL by an attacker and visited by a victim can lead to arbitrary JavaScript code execution.			21803 MISC
advantech -- r-seenet	This vulnerability is present in device_graph_page.php script, which is a part of the Advantech R-SeeNet web applications. A specially crafted URL by an attacker and visited by a victim can lead to arbitrary JavaScript code execution.	2021-07-16	4.3	CVE-2021-21802 MISC
advantech -- r-seenet	This vulnerability is present in device_graph_page.php script, which is a part of the Advantech R-SeeNet web applications. A specially crafted URL by an attacker and visited by a victim can lead to arbitrary JavaScript code execution.	2021-07-16	4.3	CVE-2021-21801 MISC
dlink -- dir-3040_firmware	A hard-coded password vulnerability exists in the Zebra IP Routing Manager functionality of D-LINK DIR-3040 1.13B03. A specially crafted network request can lead to a denial of service. An attacker can send a sequence of requests to trigger this vulnerability.	2021-07-16	5	CVE-2021-21818 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dlink -- dir-3040_firmware	An information disclosure vulnerability exists in the Zebra IP Routing Manager functionality of D-LINK DIR-3040 1.13B03. A specially crafted network request can lead to the disclosure of sensitive information. An attacker can send a sequence of requests to trigger this vulnerability.	2021-07-16	5	CVE-2021-21817 MISC
dlink -- dir-3040_firmware	A code execution vulnerability exists in the Libcli Test Environment functionality of D-LINK DIR-3040 1.13B03. A specially crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger this vulnerability.	2021-07-16	6.5	CVE-2021-21819 MISC
microsoft -- 365_apps	Microsoft Word Remote Code Execution Vulnerability	2021-07-16	6.8	CVE-2021-34452 MISC
microsoft -- office_online_server	Microsoft Office Online Server Spoofing Vulnerability	2021-07-16	5	CVE-2021-34451 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- sharepoint_foundation	Microsoft SharePoint Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34468, CVE-2021-34520.	2021-07-16	6.5	CVE-2021-34467 MISC
microsoft -- windows	Windows Print Spooler Elevation of Privilege Vulnerability	2021-07-16	4.6	CVE-2021-34481 MISC
microsoft -- windows_10	Windows MSHTML Platform Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34497.	2021-07-16	6.8	CVE-2021-34447 MISC
microsoft -- windows_10	Windows HTML Platforms Security Feature Bypass Vulnerability	2021-07-16	6.8	CVE-2021-34446 MISC
microsoft -- windows_10	Windows AppX Deployment Extensions Elevation of Privilege Vulnerability	2021-07-16	4.6	CVE-2021-34462

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
microsoft -- windows_10	Windows Container Isolation FS Filter Driver Elevation of Privilege Vulnerability	2021-07-16	4.6	CVE-2021-34461 MISC
microsoft -- windows_10	Storage Spaces Controller Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33751, CVE-2021-34510, CVE-2021-34512, CVE-2021-34513.	2021-07-16	4.6	CVE-2021-34460 MISC
microsoft -- windows_10	Microsoft Windows Media Foundation Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34439, CVE-2021-34503.	2021-07-16	6.8	CVE-2021-34441 MISC
microsoft -- windows_10	Windows AppContainer Elevation Of Privilege Vulnerability	2021-07-16	4.6	CVE-2021-34459 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33761, CVE-2021-33773, CVE-2021-34445.	2021-07-16	4.6	CVE-2021-34456 MISC
microsoft -- windows_10	Windows File History Service Elevation of Privilege Vulnerability	2021-07-16	4.6	CVE-2021-34455 MISC
microsoft -- windows_10	Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-34516.	2021-07-16	4.6	CVE-2021-34449 MISC
microsoft -- windows_10	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33761, CVE-2021-33773, CVE-2021-34456.	2021-07-16	4.6	CVE-2021-34445 MISC
microsoft -- windows_10	Windows Font Driver Host Remote Code Execution Vulnerability	2021-07-16	6.8	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				34438 MISC
microsoft -- windows_server_2008	Windows DNS Server Denial of Service Vulnerability This CVE ID is unique from CVE-2021-33745, CVE-2021-34442, CVE-2021-34499.	2021-07-16	4	CVE-2021-34444 MISC
microsoft -- windows_server_2008	Windows DNS Server Denial of Service Vulnerability This CVE ID is unique from CVE-2021-33745, CVE-2021-34444, CVE-2021-34499.	2021-07-16	5	CVE-2021-34442 MISC
mikrotik -- routeros	Mikrotik RouterOs before stable 6.47 suffers from an uncontrolled resource consumption in the sshd process. An authenticated remote attacker can cause a Denial of Service due to overloading the systems CPU.	2021-07-19	4	CVE-2020-20230 MISC
mikrotik -- routeros	Mikrotik RouterOs before stable 6.47 suffers from an uncontrolled resource consumption in the memtest process. An authenticated remote	2021-07-19	4	CVE-2020-20248 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker can cause a Denial of Service due to overloading the systems CPU.			
oracle -- access_manager	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Rest interfaces for Access Mgr). The supported version that is affected is 11.1.2.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTPS to compromise Oracle Access Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Access Manager accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	2021-07-21	4	CVE-2021-2358 MISC
oracle -- advanced_inbound_telephony	Vulnerability in the Oracle Advanced Inbound Telephony product of Oracle E-Business Suite (component: SDK client integration). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged	2021-07-21	5.5	CVE-2021-2361 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker with network access via HTTP to compromise Oracle Advanced Inbound Telephony. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Advanced Inbound Telephony accessible data as well as unauthorized access to critical data or complete access to all Oracle Advanced Inbound Telephony accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).			
oracle -- advanced_outbound_telephony	Vulnerability in the Oracle Advanced Outbound Telephony product of Oracle E-Business Suite (component: Region Mapping). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Advanced Outbound Telephony. Successful attacks of this vulnerability can result in unauthorized	2021-07-21	5.5	CVE-2021-2398 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	creation, deletion or modification access to critical data or all Oracle Advanced Outbound Telephony accessible data as well as unauthorized access to critical data or complete access to all Oracle Advanced Outbound Telephony accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).			
oracle -- application_express	Vulnerability in the Oracle Application Express Data Reporter component of Oracle Database Server. The supported version that is affected is Prior to 21.1.0.00.04. Easily exploitable vulnerability allows low privileged attacker having Valid User Account privilege with network access via HTTP to compromise Oracle Application Express Data Reporter. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express Data Reporter, attacks may significantly impact additional products. Successful attacks of this vulnerability can	2021-07-21	4.9	CVE-2021-2460 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	result in unauthorized update, insert or delete access to some of Oracle Application Express Data Reporter accessible data as well as unauthorized read access to a subset of Oracle Application Express Data Reporter accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).			
oracle -- applications_framework	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Attachments / File Upload). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Framework, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access	2021-07-21	4.9	CVE-2021-2380 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to critical data or complete access to all Oracle Applications Framework accessible data as well as unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).			
oracle -- approvals_management	Vulnerability in the Oracle Approvals Management product of Oracle E-Business Suite (component: AME Page rendering). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Approvals Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Approvals Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Approvals Management accessible data. CVSS 3.1 Base	2021-07-21	5.5	CVE-2021-2360 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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).			
oracle -- bi_publisher	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: E-Business Suite - XDO). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle BI Publisher accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2021-07-21	5	CVE-2021-2401 MISC MISC
oracle -- bi_publisher	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: E-Business Suite - XDO). Supported versions that are affected are	2021-07-21	5	CVE-2021-2400

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).			MISC MISC
oracle -- coherence	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle Coherence. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Coherence. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector:	2021-07-21	5	CVE-2021-2371 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).			
oracle -- coherence	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle Coherence. Successful attacks of this vulnerability can result in takeover of Oracle Coherence. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2021-07-21	6.8	CVE-2021-2428 MISC
oracle -- coherence	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle	2021-07-21	5	CVE-2021-2344 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Coherence. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Coherence. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).			
oracle -- collaborative_planning	Vulnerability in the Oracle Collaborative Planning product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Collaborative Planning. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Collaborative Planning accessible data as well as unauthorized access to critical data or complete access to all Oracle Collaborative Planning accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity	2021-07-21	5.5	CVE-2021-2406 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).			
oracle -- commerce_experience_manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Tools and Frameworks). The supported version that is affected is 11.3.1.5. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized read access to a subset of Oracle	2021-07-21	4.9	CVE-2021-2346 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).			
oracle -- commerce_experience_manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Tools and Frameworks). The supported version that is affected is 11.3.1.5. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Guided	2021-07-21	4.9	CVE-2021-2345 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Search / Oracle Commerce Experience Manager accessible data as well as unauthorized read access to a subset of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).			
oracle -- commerce_service_center	Vulnerability in the Oracle Commerce Service Center product of Oracle Commerce (component: Commerce Service Center). Supported versions that are affected are 11.0.0, 11.1.0, 11.2.0 and 11.3.0-11.3.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Service Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Service Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete	2021-07-21	5.8	CVE-2021-2462 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	access to some of Oracle Commerce Service Center accessible data as well as unauthorized read access to a subset of Oracle Commerce Service Center accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).			
oracle -- core_rdbms	Vulnerability in the Core RDBMS component of Oracle Database Server. The supported version that is affected is 19c. Easily exploitable vulnerability allows low privileged attacker having Create Table privilege with network access via Oracle Net to compromise Core RDBMS. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Core RDBMS. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	2021-07-21	4	CVE-2021-2330 MISC
oracle -- database	Vulnerability in the Oracle XML DB component of Oracle Database Server.	2021-07-21	6.5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Any Procedure, Create Public Synonym privilege with network access via Oracle Net to compromise Oracle XML DB. Successful attacks of this vulnerability can result in takeover of Oracle XML DB. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).			2337 MISC
oracle -- database_vault	Vulnerability in the Database Vault component of Oracle Database Server. Supported versions that are affected are 12.2.0.1 and 19c. Easily exploitable vulnerability allows high privileged attacker having DBA privilege with network access via Oracle Net to compromise Database Vault. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Database Vault accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector:	2021-07-21	4	CVE-2021-2326 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:L/I:N/A:N).			
oracle -- engineering	Vulnerability in the Oracle Engineering product of Oracle E-Business Suite (component: Change Management). Supported versions that are affected are 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Engineering. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Engineering accessible data as well as unauthorized access to critical data or complete access to all Oracle Engineering accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-07-21	5.5	CVE-2021-2405 MISC
oracle -- field_service	Vulnerability in the Oracle Field Service product of Oracle E-Business Suite (component: Wireless). Supported versions	2021-07-21	5.5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Field Service. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Field Service accessible data as well as unauthorized access to critical data or complete access to all Oracle Field Service accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).			2362 MISC
oracle -- flexcube_universal_banking	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Loans And Deposits). Supported versions that are affected are 12.0-12.4, 14.0-14.4 and . Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the	2021-07-21	4.9	CVE-2021-2324 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N).			
oracle -- flexcube_universal_banking	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Flex-Branch). Supported versions that are affected are 12.3, 12.4, 14.0-14.4 and . Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.1 Base Score 5.9	2021-07-21	4.3	CVE-2021-2323 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).			
oracle -- graalvm	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u301, 8u291, 11.0.11, 16.0.1; Oracle GraalVM Enterprise Edition: 20.3.2 and 21.1.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This	2021-07-21	4.3	CVE-2021-2341 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).			
oracle -- graalvm	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Library). Supported versions that are affected are Java SE: 7u301, 8u291, 11.0.11, 16.0.1; Oracle GraalVM Enterprise Edition: 20.3.2 and 21.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running	2021-07-21	4.3	CVE-2021-2369 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).			
oracle -- hyperion_essbase_administration_services	Vulnerability in the Hyperion Essbase Administration Services product of Oracle Essbase (component: EAS Console). Supported versions that are affected are 11.1.2.4 and 21.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Hyperion Essbase Administration Services. While the vulnerability is in Hyperion Essbase Administration Services, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or	2021-07-21	5	CVE-2021-2349 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	complete access to all Hyperion Essbase Administration Services accessible data. CVSS 3.1 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).			
oracle -- hyperion_essbase_administration_services	Vulnerability in the Hyperion Essbase Administration Services product of Oracle Essbase (component: EAS Console). Supported versions that are affected are 11.1.2.4 and 21.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Hyperion Essbase Administration Services. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Hyperion Essbase Administration Services accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2021-07-21	5	CVE-2021-2350 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- hyperion_infrastructure_technology	Vulnerability in the Hyperion Infrastructure Technology product of Oracle Hyperion (component: Lifecycle Management). The supported version that is affected is 11.2.5.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Hyperion Infrastructure Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Hyperion Infrastructure Technology accessible data as well as unauthorized update, insert or delete access to some of Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 5.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:L/A:N).	2021-07-21	4.9	CVE-2021-2347 MISC
oracle -- identity_manager	Vulnerability in the Identity Manager product of Oracle Fusion Middleware (component: Request Management & Workflow). The supported version that is affected is 11.1.2.3.0.	2021-07-21	5	CVE-2021-2457 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Identity Manager. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Identity Manager accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).			
oracle -- identity_manager	Vulnerability in the Identity Manager product of Oracle Fusion Middleware (component: Identity Console). Supported versions that are affected are 11.1.2.2.0, 11.1.2.3.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Identity Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Identity Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all	2021-07-21	4.9	CVE-2021-2458 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Identity Manager accessible data as well as unauthorized update, insert or delete access to some of Identity Manager accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).			
oracle -- jd_edwards_enterpriseone_tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime). Supported versions that are affected are 9.2.5.3 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards	2021-07-21	5.8	CVE-2021-2375 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).			
oracle -- jd_edwards_enterpriseone_tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime). Supported versions that are affected are 9.2.5.3 and Prior. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and	2021-07-21	4.9	CVE-2021-2373 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).			
oracle -- marketing	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2021-07-21	5.8	CVE-2021-2359 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- marketing	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Marketing accessible data as well as unauthorized access to critical data or complete access to all Oracle Marketing accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2021-07-21	6.4	CVE-2021-2355 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Memcached). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via	2021-07-21	4	CVE-2021-2340 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 partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).			
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	6.8	CVE-2021-2339 MISC CONFIRM

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 5.7.34 and prior and 8.0.25 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:H).	2021-07-21	4.9	CVE-2021-2356 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Federated). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL	2021-07-21	6.8	CVE-2021-2354 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	4	CVE-2021-2357 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	6.8	CVE-2021-2352 MISC CONFIRM
oracle -- mysql_cluster	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: JS module). Supported versions that are affected are 8.0.25 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Cluster. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster.	2021-07-21	4.3	CVE-2021-2411 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).			
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.34 and prior and 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	4	CVE-2021-2342 MISC
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily	2021-07-21	4	CVE-2021-2367 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).			CONFIRM
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector:	2021-07-21	4	CVE-2021-2370 MISC CONFIRM

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_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	4	CVE-2021-2399 MISC CONFIRM
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Locking). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this	2021-07-21	4	CVE-2021-2402 MISC CONFIRM

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_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.34 and prior and 8.0.25 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).	2021-07-21	4.9	CVE-2021-2385 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	4	CVE-2021-2412 MISC CONFIRM
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash	2021-07-21	4	CVE-2021-2422 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(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_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	4	CVE-2021-2424 MISC CONFIRM
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are	2021-07-21	4	CVE-2021-2425

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).			MISC CONFIRM
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS	2021-07-21	4	CVE-2021-2426 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).			
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	4	CVE-2021-2427 MISC CONFIRM
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high	2021-07-21	4	CVE-2021-2410 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 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).			CONFIRM
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note:	2021-07-21	5.8	CVE-2021-2431 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N).			
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as	2021-07-21	5.8	CVE-2021-2452 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N).			
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to	2021-07-21	5.8	CVE-2021-2453 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N).			
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this	2021-07-21	5.8	CVE-2021-2430 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N).			
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Difficult to exploit vulnerability allows unauthenticated attacker with network access	2021-07-21	5.8	CVE-2021-2450 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N).			
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5.	2021-07-21	5.8	CVE-2021-2451 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N).			
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion	2021-07-21	5.8	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N).			2423 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N).	2021-07-21	5.8	CVE-2021-2449 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- peoplesoft_enterprise_hcm_candidate_gateway	Vulnerability in the PeopleSoft Enterprise HCM Candidate Gateway product of Oracle PeopleSoft (component: e-mail notification). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Candidate Gateway. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HCM Candidate Gateway accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HCM Candidate Gateway accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2021-07-21	6.4	CVE-2021-2404 MISC
oracle -- peoplesoft_enterprise_hcm_shared_components	Vulnerability in the PeopleSoft Enterprise HCM Shared Components product of Oracle PeopleSoft (component: Person Search). The supported version that is affected is 9.2. Easily exploitable vulnerability allows high	2021-07-21	5.5	CVE-2021-2455 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Shared Components. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise HCM Shared Components accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise HCM Shared Components accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N).			
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.57, 8.58 and 8.59. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft	2021-07-21	5	CVE-2021-2407 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).			
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: SQR). Supported versions that are affected are 8.57, 8.58 and 8.59. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2021-07-21	4	CVE-2021-2377 MISC
oracle -- peoplesoft_enterprise_pt_peopletools	Vulnerability in the PeopleSoft Enterprise PT PeopleTools product of Oracle PeopleSoft (component: Notification Configuration). The	2021-07-21	5.8	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	supported version that is affected is 8.59. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PT PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PT PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PT PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).			2408 MISC
oracle -- public_sector_financials	Vulnerability in the Oracle Public Sector Financials (International) product of Oracle E-Business Suite (component: Authorization). Supported versions that are affected are	2021-07-21	5.5	CVE-2021-2363 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Public Sector Financials (International). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Public Sector Financials (International) accessible data as well as unauthorized access to critical data or complete access to all Oracle Public Sector Financials (International) accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).			
oracle -- secure_global_desktop	Vulnerability in the Oracle Secure Global Desktop product of Oracle Virtualization (component: Server). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle Secure Global Desktop. While the vulnerability is in Oracle Secure	2021-07-21	6.5	CVE-2021-2447 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Global Desktop, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Secure Global Desktop. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).			
oracle -- secure_global_desktop	Vulnerability in the Oracle Secure Global Desktop product of Oracle Virtualization (component: Client). The supported version that is affected is 5.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Secure Global Desktop. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Secure Global Desktop, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Secure Global Desktop. CVSS 3.1 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector:	2021-07-21	6.8	CVE-2021-2446 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:H/A:H).			
oracle -- siebel_marketing	Vulnerability in the Siebel Apps - Marketing product of Oracle Siebel CRM (component: Email Marketing Stand-Alone). Supported versions that are affected are 21.5 and Prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel Apps - Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Siebel Apps - Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Siebel Apps - Marketing accessible data as well as unauthorized read access to a subset of Siebel Apps - Marketing accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2021-07-21	5.8	CVE-2021-2338 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- text	Vulnerability in the Oracle Text component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Any Procedure, Alter Any Table privilege with network access via Oracle Net to compromise Oracle Text. Successful attacks of this vulnerability can result in takeover of Oracle Text. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2021-07-21	6.5	CVE-2021-2328 MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.24. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products.	2021-07-21	4.6	CVE-2021-2409 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).			
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.24. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox as well as unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data and unauthorized read access to a subset	2021-07-21	4.6	CVE-2021-2443 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	of Oracle VM VirtualBox accessible data. Note: This vulnerability applies to Solaris x86 and Linux systems only. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:H).			
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.24. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2021-07-21	4.4	CVE-2021-2454 MISC
oracle -- web_applications_desktop_integrator	Vulnerability in the Oracle Web Applications Desktop Integrator product of Oracle E-	2021-07-21	5.5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Business Suite (component: Application Service). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Web Applications Desktop Integrator. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Web Applications Desktop Integrator accessible data as well as unauthorized access to critical data or complete access to all Oracle Web Applications Desktop Integrator accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).			2434 MISC
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, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and	2021-07-21	5	CVE-2021-2376 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).			
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 T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS	2021-07-21	5	CVE-2021-2378 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).			
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 impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2021-07-21	5	CVE-2021-2403 MISC
oracle -- workflow	Vulnerability in the Oracle Workflow product of Oracle E-Business Suite (component: Workflow Notification Mailer). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability	2021-07-21	4	CVE-2021-2343 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allows low privileged attacker with network access via HTTP to compromise Oracle Workflow. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Workflow accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).			
oracle -- xml_database	Vulnerability in the Oracle XML DB component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Easily exploitable vulnerability allows high privileged attacker having Alter User privilege with network access via Oracle Net to compromise Oracle XML DB. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle XML DB accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	2021-07-21	4	CVE-2021-2333 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- xml_database	Vulnerability in the Oracle XML DB component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Any Procedure, Create Public Synonym privilege with network access via Oracle Net to compromise Oracle XML DB. Successful attacks of this vulnerability can result in takeover of Oracle XML DB. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2021-07-21	6.5	CVE-2021-2329 MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
blackboard -- blackboard_learn	Blackboard Learn through 9.1 allows XSS by an authenticated user via the Feedback to Learner form.	2021-07-20	3.5	CVE-2021-36747 MISC
blackboard -- blackboard_learn	Blackboard Learn through 9.1 allows XSS by an authenticated user via the Assignment Instructions HTML editor.	2021-07-20	3.5	CVE-2021-36746 MISC
microsoft -- windows_10	Windows Hello Security Feature Bypass Vulnerability	2021-07-16	3.6	CVE-2021-34466 MISC
microsoft -- windows_10	GDI+ Information Disclosure Vulnerability	2021-07-16	2.1	CVE-2021-34440 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	Windows Remote Access Connection Manager Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-33763, CVE-2021-34457.	2021-07-16	2.1	CVE-2021-34454 MISC
microsoft -- windows_10	Windows Remote Access Connection Manager Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-33763, CVE-2021-34454.	2021-07-16	2.1	CVE-2021-34457 MISC
oracle -- database	Vulnerability in the Oracle Database - Enterprise Edition Data Redaction component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Oracle Database - Enterprise Edition Data Redaction. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of	2021-07-21	3.5	CVE-2021-2334 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Oracle Database - Enterprise Edition Data Redaction accessible data. CVSS 3.1 Base Score 3.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N).			
oracle -- database	Vulnerability in the Oracle Database - Enterprise Edition Data Redaction component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Oracle Database - Enterprise Edition Data Redaction. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Database - Enterprise Edition Data Redaction accessible data. CVSS 3.1 Base Score 3.5 (Integrity impacts). CVSS	2021-07-21	3.5	CVE-2021-2335 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N).			
oracle -- database	Vulnerability in the Oracle Database - Enterprise Edition Data Redaction component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Oracle Database - Enterprise Edition Data Redaction. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Database - Enterprise Edition Data Redaction accessible data. CVSS 3.1 Base Score 3.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N).	2021-07-21	3.5	CVE-2021-2336 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- financial_services_crime_and_compliance_investigation_hub	Vulnerability in the Oracle Financial Services Crime and Compliance Investigation Hub product of Oracle Financial Services Applications (component: Reports). The supported version that is affected is 20.1.2. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Financial Services Crime and Compliance Investigation Hub executes to compromise Oracle Financial Services Crime and Compliance Investigation Hub. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Crime and Compliance Investigation Hub, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Crime and Compliance Investigation Hub accessible data as well as unauthorized read access to a subset of Oracle Financial Services Crime and	2021-07-21	2.6	CVE-2021-2448 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Compliance Investigation Hub accessible data. CVSS 3.1 Base Score 3.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:C/C:L/I:L/A:N).			
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.34 and prior and 8.0.25 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	3.5	CVE-2021-2372 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.25 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N).	2021-07-21	1.9	CVE-2021-2374 MISC CONFIRM
oracle -- siebel_core_-_server_framework	Vulnerability in the Siebel Core - Server Framework product of Oracle Siebel CRM (component: Loging). Supported versions that are affected are 21.5 and Prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Siebel Core - Server Framework executes to compromise	2021-07-21	2.1	CVE-2021-2353 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Siebel Core - Server Framework. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel Core - Server Framework accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).			
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 infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle	2021-07-21	3.3	CVE-2021-2381 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Solaris. CVSS 3.1 Base Score 3.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L).			
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.24. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 6.0 (Availability impacts). CVSS Vector:	2021-07-21	2.1	CVE-2021-2442 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H).			