Oracle Critical Patch Update Advisory - April 2020

Description

A Critical Patch Update is a collection of patches for multiple security vulnerabilities. These patches are usually cumulative, but each advisory describes only the security patches added since the previous Critical Patch Update advisory. Thus, prior Critical Patch Update advisories should be reviewed for information regarding earlier published security patches. Please refer to:

- Critical Patch Updates, Security Alerts and Bulletins for information about Oracle Security Advisories.

Oracle continues to periodically receive reports of attempts to maliciously exploit vulnerabilities for which Oracle has already released security patches. In some instances, it has been reported that attackers have been successful because targeted customers had failed to apply available Oracle patches. Oracle therefore strongly recommends that customers remain on actively-supported versions and apply Critical Patch Update security patches without delay.

This Critical Patch Update contains 399 new security patches across the product families listed below. Please note that an MOS note summarizing the content of this Critical Patch Update and other Oracle Software Security Assurance activities is located at April 2020 Critical Patch Update: Executive Summary and Analysis.

Affected Products and Patch Information

Security vulnerabilities addressed by this Critical Patch Update affect the products listed below. The product area is shown in the Patch Availability Document column.

Please click on the links in the Patch Availability Document column below to access the documentation for patch availability information and installation instructions.

Affected Products and Versions	Patch Availability Document
Application Performance Management, versions 12.1.0.5, 13.2.0.0, 13.3.0.0	Enterprise Manager

Affected Products and Versions	Patch Availability Document
Application Service Level Management, versions 13.2.0.0, 13.3.0.0	Enterprise Manager
Enterprise Manager Base Platform, versions 12.1.0.5, 13.2.0.0, 13.3.0.0	Enterprise Manager
Hyperion Financial Management, version 11.1.2.4	Fusion Middleware
Hyperion Financial Reporting, version 11.1.2.4	Fusion Middleware
Identity Manager Connector, version 9.0	Fusion Middleware
Instantis EnterpriseTrack, versions 17.1-17.3	Oracle Construction and Engineering Suite
Java Advanced Management Console, version 2.16	Java SE
JD Edwards EnterpriseOne Tools, version 9.2	JD Edwards
JD Edwards World Security, versions A9.3, A9.3.1, A9.4	JD Edwards
MICROS Relate CRM Software, version 11.4	Retail Applications
MySQL Client, versions 5.6.47 and prior, 5.7.29 and prior, 8.0.18 and prior	MySQL
MySQL Cluster, versions 7.3.28 and prior, 7.4.27 and prior, 7.5.17 and prior, 7.6.13 and prior, 8.0.19 and prior	MySQL
MySQL Connectors, versions 5.1.48 and prior, 8.0.19 and prior	MySQL
MySQL Enterprise Monitor, versions 4.0.11.5331 and prior, 8.0.18.1217 and prior	MySQL
MySQL Server, versions 5.6.47 and prior, 5.7.29 and prior, 8.0.19 and prior	MySQL
MySQL Workbench, versions 8.0.19 and prior	MySQL
Oracle Access Manager, versions 11.1.2.3.0, 12.2.1.3.0	Fusion Middleware
Oracle Agile PLM, versions 9.3.3, 9.3.5, 9.3.6	Oracle Supply Chain Products
Oracle API Gateway, version 11.1.2.4.0	Fusion Middleware
Oracle Application Express, versions prior to 19.2	Database
Oracle Application Testing Suite, versions 13.2.0.1, 13.3.0.1	Enterprise Manager
Oracle Banking Enterprise Collections, versions 2.7.0, 2.8.0	Oracle Banking Platform
Oracle Banking Enterprise Originations, versions 2.7.0, 2.8.0	Oracle Banking Platform
Oracle Banking Enterprise Product Manufacturing, versions 2.7.0, 2.8.0	Oracle Banking Platform
Oracle Banking Platform, versions 2.4.0, 2.4.1, 2.5.0, 2.6.0, 2.6.1, 2.6.2, 2.7.0, 2.7.1, 2.9.0	Oracle Banking Platform
Oracle Big Data Discovery, version 1.6	Fusion Middleware

Affected Products and Versions	Patch Availability Document
Oracle Business Intelligence Enterprise Edition, versions 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Business Process Management Suite, version 12.2.1.4.0	Fusion Middleware
Oracle Coherence, versions 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Communications ASAP Cartridges, versions 7.2, 7.3	Oracle Communications ASAP Cartridges
Oracle Communications Calendar Server, versions 8.0.0.2.0, 8.0.0.3.0	Oracle Communications Calendar Se
Oracle Communications Converged Application Server - Service Controller, version 6.1	Oracle Communications Converged Application Server - Service Controlle
Oracle Communications Diameter Signaling Router (DSR), versions 8.0.0, 8.1.0, 8.2.0, 8.2.1	Oracle Communications Diameter Signaling Router
Oracle Communications Element Manager, versions 8.0.0, 8.1.0, 8.1.1, 8.2.0	Oracle Communications Element Manager
Oracle Communications Evolved Communications Application Server, version 7.1	Oracle Communications Evolved Communications Application Server
Oracle Communications Messaging Server, versions 8.0.2, 8.1.0	Oracle Communications Messaging Server
Oracle Communications Operations Monitor, versions 3.4.0, 4.0.0, 4.1.0, 4.2.0, 4.3.0	Oracle Communications Operations Monitor
Oracle Communications Service Broker, versions 6.0, 6.1	Oracle Communications Service Brok
Oracle Communications Services Gatekeeper, versions 6.0, 6.1	Oracle Communications Services Gatekeeper
Oracle Communications Session Report Manager, versions 8.0.0, 8.1.0, 8.1.1, 8.2.0	Oracle Communications Session Rep Manager
Oracle Communications Session Route Manager, versions 8.0.0, 8.1.0, 8.1.1, 8.2.0	Oracle Communications Session Rou Manager
Oracle Communications Unified Inventory Management, versions 7.3.0, 7.4.0	Oracle Communications Unified Inventory Management
Oracle Communications WebRTC Session Controller, version 7.2	Oracle Communications WebRTC Session Controller
Oracle Configurator, versions 12.1, 12.2	Oracle Supply Chain Products
Oracle Database Server, versions 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c, 19c	Database
Oracle E-Business Suite, versions 12.1.1-12.1.3, 12.2.3-12.2.9	E-Business Suite
Oracle Endeca Information Discovery Integrator, version 3.2.0	Fusion Middleware
Oracle Endeca Server, version 7.7.0	Fusion Middleware

Affected Products and Versions	Patch Availability Document
Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.6-8.0.9	Oracle Financial Services Analytical Applications Infrastructure
Oracle Financial Services Asset Liability Management, versions 8.0.6, 8.0.7	Oracle Financial Services Asset Liabil Management
Oracle Financial Services Balance Sheet Planning, version 8.0.8	Oracle Financial Services Balance Sh Planning
Oracle Financial Services Data Foundation, versions 8.0.6-8.0.9	Oracle Financial Services Data Foundation
Oracle Financial Services Deposit Insurance Calculations for Liquidity Risk Management, versions 8.0.7, 8.0.8	Oracle Financial Services Deposit Insurance Calculations for Liquidity F Management
Oracle Financial Services Funds Transfer Pricing, versions 8.0.6, 8.0.7	Oracle Financial Services Funds Tran Pricing
Oracle Financial Services Hedge Management and IFRS Valuations, versions 8.0.6-8.0.8	Oracle Financial Services Hedge Management and IFRS Valuations
Oracle Financial Services Liquidity Risk Management, version 8.0.6	Oracle Financial Services Liquidity Ri Management
Oracle Financial Services Liquidity Risk Measurement and Management, versions 8.0.7, 8.0.8	Oracle Financial Services Liquidity Ri Measurement and Management
Oracle Financial Services Loan Loss Forecasting and Provisioning, versions 8.0.6-8.0.8	Oracle Financial Services Loan Loss Forecasting and Provisioning
Oracle Financial Services Market Risk Measurement and Management, versions 8.0.6, 8.0.8	Oracle Financial Services Market Risk Measurement and Management
Oracle Financial Services Price Creation and Discovery, version 8.0.7	Oracle Financial Services Price Creati And Discovery
Oracle Financial Services Profitability Management, versions 8.0.6, 8.0.7	Oracle Financial Services Profitability Management
Oracle Financial Services Revenue Management and Billing Analytics, versions 2.6, 2.7, 2.8	Oracle Financial Services Revenue Management and Billing Analytics
Oracle FLEXCUBE Core Banking, version 4.0	Oracle Financial Services Application
Oracle FLEXCUBE Private Banking, versions 12.0, 12.1	Oracle Financial Services Application
Oracle Fusion Middleware MapViewer, version 12.2.1.3.0	Fusion Middleware
Oracle Global Lifecycle Management NextGen OUI Framework, versions 12.2.1.3.0, 12.2.1.4.0, 13.9.4.2.2	Fusion Middleware
Oracle Global Lifecycle Management OPatch, versions prior to 11.2.0.3.23, prior to 12.2.0.1.19, prior to 13.9.4.2.1	Global Lifecycle Management
Oracle GraalVM Enterprise Edition, versions 19.3.1, 20.0.0	Oracle GraalVM Enterprise Edition
Oracle Health Sciences Information Manager, version 3.0	Health Sciences

Affected Products and Versions	Patch Availability Document
Oracle Healthcare Data Repository, version 7.0	Health Sciences
Oracle Hospitality Reporting and Analytics, version 9.1.0	Oracle Hospitality Reporting and Analytics
Oracle HTTP Server, version 11.1.1.9.0	Fusion Middleware
Oracle In-Memory Performance-Driven Planning, versions 12.1, 12.2	Oracle Supply Chain Products
Oracle Insurance Accounting Analyzer, versions 8.0.6-8.0.9	Oracle Insurance Accounting Analyze
Oracle Java SE, versions 7u251, 8u241, 11.0.6, 14	Java SE
Oracle Java SE Embedded, version 8u241	Java SE
Oracle Knowledge, versions 8.6.0-8.6.3	Oracle Knowledge
Oracle Managed File Transfer, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Outside In Technology, versions 8.5.4	Fusion Middleware
Oracle Real User Experience Insight, versions 13.1.2.1, 13.2.3.1, 13.3.1.0	Enterprise Manager
Oracle Retail Advanced Inventory Planning, versions 14.0, 15.0, 16.0	Retail Applications
Oracle Retail Back Office, version 14.1	Retail Applications
Oracle Retail Central Office, version 14.1	Retail Applications
Oracle Retail Customer Management and Segmentation Foundation, version 18.0	Retail Applications
Oracle Retail Merchandising System, version 16.0	Retail Applications
Oracle Retail Order Broker, versions 15.0, 16.0, 18.0, 19.0	Retail Applications
Oracle Retail Point-of-Service, version 14.1	Retail Applications
Oracle Retail Predictive Application Server, versions 15.0.3, 16.0.3	Retail Applications
Oracle Retail Returns Management, version 14.1	Retail Applications
Oracle Retail Store Inventory Management, version 16.0	Retail Applications
Oracle Retail Xstore Point of Service, versions 7.1, 15.0, 16.0, 17.0, 18.0, 18.0.1	Retail Applications
Oracle SD-WAN Edge, versions 7.3, 8.0, 8.1, 8.2	Oracle SD-WAN Edge
Oracle Secure Backup, versions prior to 18.1	Oracle Secure Backup
Oracle SOA Suite, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Solaris, versions 10, 11	Systems
Oracle Transportation Management, versions 6.3.7, 6.4.2, 6.4.3	Oracle Supply Chain Products

Affected Products and Versions	Patch Availability Document
Oracle Unified Directory, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle Utilities Framework, versions 2.2.0, 4.2.0.2, 4.2.0.3, 4.3.0.2-4.3.0.6, 4.4.0.0, 4.4.0.2	Oracle Utilities Applications
Oracle Utilities Network Management System, versions 1.12.0.3, 2.3.0.1, 2.3.0.2, 2.4.0.0	Oracle Utilities Applications
Oracle VM VirtualBox, versions prior to 5.2.40, prior to 6.0.20, prior to 6.1.6	Virtualization
Oracle WebCenter Portal, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle WebCenter Sites, versions 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle WebLogic Server, versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0	Fusion Middleware
Oracle ZFS Storage Appliance Kit, version 8.8	Systems
OSS Support Tools, versions 20.0, 20.1	Support Tools
PeopleSoft Enterprise CS Campus Community, version 9.2	PeopleSoft
PeopleSoft Enterprise HCM Absence Management, version 9.2	PeopleSoft
PeopleSoft Enterprise HRMS, version 9.2	PeopleSoft
PeopleSoft Enterprise PeopleTools, versions 8.56, 8.57, 8.58	PeopleSoft
PeopleSoft Enterprise SCM Purchasing, version 9.2	PeopleSoft
Primavera Gateway, versions 16.2.0-16.2.11, 17.12.0-17.12.6, 18.8.0-18.8.8, 19.12.0	Oracle Construction and Engineering Suite
Primavera P6 Enterprise Project Portfolio Management, versions 16.2.0.0-16.2.19.3, 17.12.0.0-17.12.17.0, 18.8.0.0-18.8.18.0, 19.12.1.0-19.12.3.0, 20.1.0.0-20.2.0.0	Oracle Construction and Engineering Suite
Primavera Unifier, versions 16.1, 16.2, 17.7-17.12, 18.8, 19.12	Oracle Construction and Engineering Suite
Siebel Applications, versions 20.2 and prior	Siebel
StorageTek Tape Analytics SW Tool, version 2.3.0	Systems

Note:

- Vulnerabilities affecting either Oracle Database or Oracle Fusion Middleware may affect Oracle Fusion Applications, so Oracle customers should refer to Oracle Fusion Applications Critical Patch Update Knowledge Document, My Oracle Support Note 1967316.1 for information on patches to be applied to Fusion Application environments.
- Vulnerabilities affecting Oracle Solaris may affect Oracle ZFSSA so Oracle customers should refer to the Oracle and Sun Systems Product Suite Critical Patch Update Knowledge Document, My Oracle Support Note 2160904.1 for information on minimum revisions of

security patches required to resolve ZFSSA issues published in Critical Patch Updates and Solaris Third Party bulletins.

- Users running Java SE with a browser can download the latest release from http://java.com. Users on the Windows and Mac OS X platforms can also use automatic updates to get the latest release.

Risk Matrix Content

Risk matrices list only security vulnerabilities that are newly addressed by the patches associated with this advisory. Risk matrices for previous security patches can be found in previous Critical Patch Update advisories and Alerts. An English text version of the risk matrices provided in this document is here.

Several vulnerabilities addressed in this Critical Patch Update affect multiple products. Each vulnerability is identified by a CVE# which is a unique identifier for a vulnerability. A vulnerability that affects multiple products will appear with the same CVE# in all risk matrices. A CVE# shown in *italics* indicates that this vulnerability impacts a different product, but also has impact on the product where the italicized CVE# is listed.

Security vulnerabilities are scored using CVSS version 3.0 (see Oracle CVSS Scoring for an explanation of how Oracle applies CVSS version 3.0).

Oracle conducts an analysis of each security vulnerability addressed by a Critical Patch Update. Oracle does not disclose detailed information about this security analysis to customers, but the resulting Risk Matrix and associated documentation provide information about the type of vulnerability, the conditions required to exploit it, and the potential impact of a successful exploit. Oracle provides this information, in part, so that customers may conduct their own risk analysis based on the particulars of their product usage. For more information, see Oracle vulnerability disclosure policies.

The protocol in the risk matrix implies that all of its secure variants (if applicable) are affected as well. For example, if HTTP is listed as an affected protocol, it implies that HTTPS (if applicable) is also affected. The secure variant of a protocol is listed in the risk matrix only if it is the *only* variant affected, e.g. HTTPS will typically be listed for vulnerabilities in SSL and TLS.

Workarounds

Due to the threat posed by a successful attack, Oracle strongly recommends that customers apply Critical Patch Update security patches as soon as possible. Until you apply the Critical Patch Update patches, it may be possible to reduce the risk of successful attack by blocking network protocols required by an attack. For attacks that require certain privileges or access to certain packages, removing the privileges or the ability to access the packages from

users that do not need the privileges may help reduce the risk of successful attack. Both approaches may break application functionality, so Oracle strongly recommends that customers test changes on non-production systems. Neither approach should be considered a long-term solution as neither corrects the underlying problem.

Skipped Critical Patch Updates

Oracle strongly recommends that customers apply security patches as soon as possible. For customers that have skipped one or more Critical Patch Updates and are concerned about products that do not have security patches announced in this Critical Patch Update, please review previous Critical Patch Update advisories to determine appropriate actions.

Critical Patch Update Supported Products and Versions

Patches released through the Critical Patch Update program are provided only for product versions that are covered under the Premier Support or Extended Support phases of the Lifetime Support Policy. Oracle recommends that customers plan product upgrades to ensure that patches released through the Critical Patch Update program are available for the versions they are currently running.

Product releases that are not under Premier Support or Extended Support are not tested for the presence of vulnerabilities addressed by this Critical Patch Update. However, it is likely that earlier versions of affected releases are also affected by these vulnerabilities. As a result, Oracle recommends that customers upgrade to supported versions.

Database, Fusion Middleware, and Oracle Enterprise Manager products are patched in accordance with the Software Error Correction Support Policy explained in My Oracle Support Note 209768.1. Please review the Technical Support Policies for further guidelines regarding support policies and phases of support.

Credit Statement

The following people or organizations reported security vulnerabilities addressed by this Critical Patch Update to Oracle:

- 21superman: CVE-2020-2828
- Abdullah H. AlJaber: CVE-2020-2753
- Abdulrahman Nour of Redforce: CVE-2020-2865
- Alexander Kornbrust of Red Database Security: CVE-2020-2737, CVE-2020-2946
- Alves Christopher: CVE-2020-2752
- Andrej Simko of Accenture: CVE-2020-2794, CVE-2020-2796, CVE-2020-2810

- Andrew Hess: CVE-2020-2910
- anhdaden of STAR Labs working with Trend Micro's Zero Day Initiative: CVE-2020-2575, CVE-2020-2748, CVE-2020-2894, CVE-2020-2902, CVE-2020-2911
- Anil Aravind: CVE-2020-2864
- Bao Zhen: CVE-2020-2926
- Barakat Soror: CVE-2020-2913, CVE-2020-2914
- Barakat Soror working with Trend Micro Zero Day Initiative: CVE-2020-2907, CVE-2020-2958
- Bengt Jonsson of Uppsala University: CVE-2020-2767
- Bui Duong from Viettel Cyber Security: CVE-2020-2883, CVE-2020-2884
- Bui Quang: CVE-2020-2933
- Calvin Fong (Lord_Idiot) of STAR Labs working with Trend Micro Zero Day Initiative: CVE-2020-2748, CVE-2020-2758
- Christian Freudigmann of Daimler TSS: CVE-2020-2738
- Damian Bury: CVE-2020-2769, CVE-2020-2777
- Dan Amodio of Contrast Security: CVE-2020-2800
- Daniel Martinez Adan (aDoN90): CVE-2020-2738
- elasticheart from ICC working with Trend Micro Zero Day Initiative: CVE-2020-2741
- Esteban Montes Morales of Accenture: CVE-2020-2813
- Fangrun Li of Cloud Security Team at Qihoo 360: CVE-2020-2798, CVE-2020-2801, CVE-2020-2963
- Fatih Çelik: CVE-2020-2909
- Florian Ohlms of Daimler TSS: CVE-2020-2738
- GreenDog working with Trend Micro Zero Day Initiative: CVE-2020-2950
- JanatiIdrissi Zouhair: CVE-2020-2752
- Jang of VNPT ISC: CVE-2020-2883, CVE-2020-2884
- John Simpson of Trend Micro Security Research working with the Zero Day Initiative: CVE-2020-2882, CVE-2020-2956
- Julien Ahrens of RCE Security: CVE-2020-2870, CVE-2020-2871, CVE-2020-2872, CVE-2020-2873, CVE-2020-2874, CVE-2020-2876, CVE-2020-2877, CVE-2020-2878, CVE-2020-2879, CVE-2020-2880, CVE-2020-2881
- Juraj Somorovsky of Ruhr-University Bochum: CVE-2020-2767
- Kaki King: CVE-2020-2883
- Kasper Leigh Haabb, Secunia Research at Flexera: CVE-2020-2783, CVE-2020-2784, CVE-2020-2785, CVE-2020-2786, CVE-2020-2787

- Khaled Sakr of Malcrove: CVE-2019-2899
- khuyenn of Viettel Cyber Security: CVE-2020-2820, CVE-2020-2823, CVE-2020-2824, CVE-2020-2825, CVE-2020-2826, CVE-2020-2827, CVE-2020-2831, CVE-2020-2832, CVE-2020-2834, CVE-2020-2835, CVE-2020-2836, CVE-2020-2838, CVE-2020-2839, CVE-2020-2840, CVE-2020-2841, CVE-2020-2842, CVE-2020-2844, CVE-2020-2845, CVE-2020-2846, CVE-2020-2847, CVE-2020-2848, CVE-2020-2849, CVE-2020-2850, CVE-2020-2852, CVE-2020-2854, CVE-2020-2855, CVE-2020-2856, CVE-2020-2857, CVE-2020-2871
- Kostis Sagonas of Uppsala University: CVE-2020-2767
- Lalit Naphade: CVE-2020-2740
- Longofo of Knownsec 404 Team: CVE-2020-2798, CVE-2020-2949, CVE-2020-2963
- lufei from 0vul Team of Butian at Qi'anxin Group: CVE-2020-2869, CVE-2020-2883
- Maoxin Lin of Dbappsecurity Team: CVE-2020-2869, CVE-2020-2934
- Marc Durdin: CVE-2020-2930
- Marco Ivaldi of Media Service: CVE-2020-2771, CVE-2020-2851, CVE-2020-2944
- Marek Cybul: CVE-2020-2766
- Martin Doyhenard of Onapsis: CVE-2020-2750
- Matei "Mal" Badanoiu: CVE-2020-2869, CVE-2020-2875
- Mauro Leggieri of TRAPMINE Inc.: CVE-2020-2895
- Michal Bogdanowicz of STM Solutions: CVE-2020-2811
- Minle Chen of PingAn Galaxy Lab: CVE-2020-2798
- Nils Emmerich of ERNW : CVE-2020-2803, CVE-2020-2805
- Owais Zaman of Sabic: CVE-2020-2594, CVE-2020-2706
- Paul Fiterau Brostean of Uppsala University: CVE-2020-2767
- Pavel Cheremushkin: CVE-2020-2929, CVE-2020-2951
- Peter Dettman of cryptoworkshop.com: CVE-2020-2778
- Philippe Antoine (Telecom Nancy): CVE-2020-2752
- Piotr Domirski: CVE-2020-2745
- Quynh Le of VNPT ISC: CVE-2020-2798
- Quynh Le of VNPT ISC working with Trend Micro Zero Day Initiative: CVE-2020-2883
- r00t4dm from A-TEAM of Legendsec at Qi'anxin Group: CVE-2020-2798, CVE-2020-2829, CVE-2020-2963
- Reno Robert working with Trend Micro Zero Day Initiative: CVE-2020-2742, CVE-2020-2743, CVE-2020-2908
- Robert Merget of Ruhr-University Bochum: CVE-2020-2767

- Roger Meyer: CVE-2020-2514
- RunOu of Bangcle Security: CVE-2020-2798
- Rémi Badonnel (Telecom Nancy): CVE-2020-2752
- Samrat Das of Emirates NBD: CVE-2020-2772
- Sebastian Fuchs of NTT Security: CVE-2020-2744
- Sebastian Wlodarczyk of Optima Partners: CVE-2020-2747
- Simone Bordet of Webtide: CVE-2020-2781
- Tarun Sehgal of eSec Forte Technologies: CVE-2020-2782
- Tomasz Wisniewski: CVE-2020-2793
- Tuan Anh Nguyen of Viettel Cyber Security: CVE-2020-2789, CVE-2020-2807, CVE-2020-2808, CVE-2020-2809, CVE-2020-2815, CVE-2020-2817, CVE-2020-2818, CVE-2020-2819, CVE-2020-2820, CVE-2020-2821, CVE-2020-2822, CVE-2020-2823, CVE-2020-2824, CVE-2020-2825, CVE-2020-2826, CVE-2020-2827, CVE-2020-2831, CVE-2020-2832, CVE-2020-2833, CVE-2020-2834, CVE-2020-2835, CVE-2020-2836, CVE-2020-2837, CVE-2020-2838, CVE-2020-2839, CVE-2020-2840, CVE-2020-2841, CVE-2020-2842, CVE-2020-2843, CVE-2020-2844, CVE-2020-2845, CVE-2020-2846, CVE-2020-2847, CVE-2020-2848, CVE-2020-2849, CVE-2020-2850, CVE-2020-2852, CVE-2020-2854, CVE-2020-2855, CVE-2020-2856, CVE-2020-2857, CVE-2020-2858, CVE-2020-2860, CVE-2020-2861, CVE-2020-2863, CVE-2020-2871
- Vahagn Vardanyan: CVE-2020-2733
- Vaibhav Shukla: CVE-2020-2955
- Venustech ADLab: CVE-2020-2798, CVE-2020-2801
- Victor Rodriguez: CVE-2020-2739
- Vishnu Dev TJ working with Trend Micro's Zero Day Initiative: CVE-2020-2929
- Xingwei Lin of Ant-financial Light-Year Security Lab: CVE-2020-2905
- Xinlei Ying of Ant-financial Light-Year Security Lab: CVE-2020-2905
- Xu Yuanzhen of Alibaba Cloud Security Team: CVE-2020-2869, CVE-2020-2934
- Yu Wang of BMH Security Team: CVE-2020-2883
- ZeddYu Lu: CVE-2020-2867
- Zhan Julien: CVE-2020-2752
- Ziming Zhang from Codesafe Team of Legendsec at Qi'anxin Group: CVE-2020-2959
- Zohaib Tasneem of Sabic: CVE-2020-2594, CVE-2020-2706

Security-In-Depth Contributors

Oracle acknowledges people who have contributed to our Security-In-Depth program (see FAQ). People are acknowledged for Security-In-Depth contributions if they provide information, observations or suggestions pertaining to security vulnerability issues that result in significant modification of Oracle code or documentation in future releases, but are not of such a critical nature that they are distributed in Critical Patch Updates.

In this Critical Patch Update Advisory, Oracle recognizes the following for contributions to Oracle's Security-In-Depth program.:

- Abdullah H. AlJaber
- Andrej Simko of Accenture working with iDefense Labs
- ICHIHARA Ryohei of DMM.com LLC
- Jayson Grace of Sandia National Laboratories
- KeChen Lin of Ping An Bank Security Team
- Markus Loewe
- Mathieu Deous of Datadoghq
- Mehdi Benkaddour
- MengLiang Ji of CICITLab
- Michael Miller of Integrigy
- Raju Mogulapalli of Rheem Manufacturing
- tint0 of Viettel Cyber Security working with iDefense Labs
- Tuan Anh Nguyen of Viettel Cyber Security

On-Line Presence Security Contributors

Oracle acknowledges people who have contributed to our On-Line Presence Security program (see FAQ). People are acknowledged for contributions relating to Oracle's on-line presence if they provide information, observations or suggestions pertaining to security-related issues that result in significant modification to Oracle's on-line external-facing systems.

For this quarter, Oracle recognizes the following for contributions to Oracle's On-Line Presence Security program:

- Anton Hrytskevich
- Chetan Tiwari
- Daniel J. Grinkevich
- Faizan Ahmed

- Hamit Cibo
- Heshie Brody
- Jimmy Bruneel
- Mohamed Yaser
- r00t4dm from A-TEAM of Legendsec at Qi'anxin Group
- Robert Lee Dick
- Shriram
- Wai Yan Aung
- Yash Ahmed Quashim

Critical Patch Update Schedule

Critical Patch Updates are released on the Tuesday closest to the 17th day of January, April, July and October. The next four dates are:

- 14 July 2020
- 20 October 2020
- 19 January 2021
- 20 April 2021

References

- Oracle Critical Patch Updates, Security Alerts and Bulletins
- Critical Patch Update - April 2020 Documentation Map
- Oracle Critical Patch Updates and Security Alerts - Frequently Asked Questions
- Risk Matrix Definitions
- Use of Common Vulnerability Scoring System (CVSS) by Oracle
- English text version of the risk matrices
- CVRF XML version of the risk matrices
- Map of CVE to Advisory
- Software Error Correction Support Policy
- Oracle Lifetime support Policy
- JEP 290 Reference Blocklist Filter

Modification History

Date	Note
2020-July-20	Rev 11. Credit Statement Update.
2020-June-19	Rev 10. Credit Statement Update.
2020-June-15	Rev 9. Added note concerning the patch for CVE-2020-2801.
2020-May-27	Rev 8. Credit Statement Update.
2020-May-18	Rev 7. Updated protocol information for CVE-2020-2798, CVE-2020-2801, CVE-2020-2828, CVE-2020-2883, CVE-2020-2884 and CVE-2020-2915.
2020-May-06	Rev 6. Credit Statement Update.
2020-April-30	Rev 5. Credit Statement Update.
2020-April-24	Rev 4. Added CVE-2020-2575 for VirtualBox to the Virtualization Risk Matrix. This increases overall number of security patches to 399. The releases listed in the patch availability docum for Virtualization already include the patch for CVE-2020-2575. Updated CVSS score for CVE 2020-2894 in the Oracle Virtualization risk matrix. Modified the additional CVE list for CVE-2018-1165 in Oracle ZFS Storage Appliance Kit.
2020-April-17	Rev 3. Modified the affected versions for Oracle Outside In Technology vulnerabilities and updated the credit statement.
2020-April-16	Rev 2. Added entry in the Oracle Fusion Middleware risk matrix for Oracle WebLogic Server security patch to address CVE-2019-16943. This increases the overall number of security patches to 398. This is simply a documentation change. The patches were already listed in th patch availability document for Fusion Middleware.
2020-April-14	Rev 1. Initial Release.

Oracle Database Products Risk Matrices

This Critical Patch Update contains 10 new security patches for the Oracle Database Products divided as follows:

- 8 new security patches for Oracle Database Server.
- 1 new security patch for Oracle Global Lifecycle Management.

- 1 new security patch for Oracle Secure Backup.

Oracle Database Server Risk Matrix

This Critical Patch Update contains 8 new security patches for the Oracle Database Server. 2 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. None of these patches are applicable to client-only installations, i.e., installations that do not have the Oracle Database Server installed. The English text form of this Risk Matrix can be found here.

CVE#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VER		
					Base Score	Attack Vector	Atta Comp
CVE-2020-2735	Java VM	Create Session	Oracle Net	No	8.0	Network	Hig
CVE-2016-10251	Oracle Multimedia	Create Session	Oracle Net	No	8.0	Network	Lo
CVE-2019-17563	WLM (Apache Tomcat)	None	HTTPS	Yes	7.5	Network	Hig
CVE-2020-2737	Core RDBMS	Create Session, Execute Catalog Role	Oracle Net	No	6.4	Network	Hig
CVE-2019-2853	Oracle Text	Create Session	OracleNet	No	6.3	Network	Lo
CVE-2016-7103	Oracle Application Express	None	HTTPS	Yes	6.1	Network	Lo
CVE-2020-2514	Oracle Application Express	End User Role	HTTPS	No	4.6	Network	Lo
CVE-2020-2734	RDBMS/Optimizer	Execute on DBMS_SQLTUNE	Oracle Net	No	2.4	Network	Lo

Additional CVEs addressed are below:

- The patch for CVE-2016-7103 also addresses CVE-2015-9251 and CVE-2019-11358.
- The patch for CVE-2019-17563 also addresses CVE-2019-12418.

- The patch for CVE-2019-2853 also addresses CVE-2019-2756, CVE-2019-2759 and CVE-2019-2852.

Oracle Global Lifecycle Management Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle Global Lifecycle Management. This vulnerability is not remotely exploitable without authentication, i.e., may not be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'
CVE-2019-20330	Oracle Global Lifecycle Management OPatch	Patch Installer	HTTP	No	0.0	Network	High	Non

Notes:
1. The following CVEs addressed by this patch are not exploitable in the Oracle product, so the CVSS score is 0.0.

Additional CVEs addressed are below:
- The patch for CVE-2019-20330 also addresses CVE-2016-4000, CVE-2016-4463, CVE-2018-1000873, CVE-2018-11307, CVE-2018-12022, CVE-2018-12023, CVE-2018-1320, CVE-2018-14718, CVE-2018-14719, CVE-2018-14720, CVE-2018-14721, CVE-2018-19360, CVE-2018-19361, CVE-2018-19362, CVE-2019-12086, CVE-2019-12384, CVE-2019-14379, CVE-2019-14439, CVE-2019-14540, CVE-2019-16335 and CVE-2020-8840.

Oracle Secure Backup Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle Secure Backup. This vulnerability is remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK (s				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	Us Inte
CVE-2018-5712	Oracle Secure Backup	PHP	HTTPS	Yes	6.1	Network	Low	None	Requ

Additional CVEs addressed are below:

- The patch for CVE-2018-5712 also addresses CVE-2018-5711.

Oracle Communications Applications Risk Matrix

This Critical Patch Update contains 39 new security patches for Oracle Communications Applications. 35 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERS		
					Base Score	Attack Vector	Attac Compl
CVE-2019-16943	Oracle Communications Calendar Server	Administration (jackson-databind)	HTTP	Yes	9.8	Network	Low
CVE-2015-3253	Oracle Communications Converged Application Server - Service Controller	Admin Console (Groovy)	HTTP	Yes	9.8	Network	Low
CVE-2016-4000	Oracle Communications Diameter Signaling Router (DSR)	IDIH Visualization (Jython)	HTTP	Yes	9.8	Network	Low
CVE-2019-2729	Oracle Communications Diameter Signaling Router (DSR)	IDIH Visualization (Oracle WebLogic Server)	HTTP	Yes	9.8	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERS		
					Base Score	Attack Vector	Attac Compl
CVE-2019-14379	Oracle Communications Diameter Signaling Router (DSR)	IDIH Visualization (jackson-databind)	HTTP	Yes	9.8	Network	Low
CVE-2019-16943	Oracle Communications Evolved Communications Application Server	SDP, SCF and URD (jackson-databind)	HTTP	Yes	9.8	Network	Low
CVE-2019-5482	Oracle Communications Operations Monitor	REST API (cURL)	HTTP	Yes	9.8	Network	Low
CVE-2019-2904	Oracle Communications Service Broker	Admin Console (Application Development Framework)	HTTP	Yes	9.8	Network	Low
CVE-2019-2904	Oracle Communications Services Gatekeeper	API Management Portal (Application Development Framework)	HTTP	Yes	9.8	Network	Low
CVE-2019-10082	Oracle Communications Element Manager	Core (Apache HTTP Server)	HTTP	Yes	9.1	Network	Low
CVE-2019-10088	Oracle Communications Messaging Server	Security (Tika)	HTTP	Yes	8.8	Network	Low
CVE-2018-8039	Oracle Communications Session Report Manager	Core (Apache CXF)	HTTP	Yes	8.1	Network	High
CVE-2018-8039	Oracle Communications	Core (Apache CXF)	HTTP	Yes	8.1	Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERS		
					Base Score	Attack Vector	Attac Compl
	Session Route Manager						
CVE-2019-0211	Oracle Communications Session Report Manager	Core (Apache HTTP Server)	None	No	7.8	Local	Low
CVE-2019-0211	Oracle Communications Session Route Manager	Core (Apache HTTP Server)	None	No	7.8	Local	Low
CVE-2019-0227	Oracle Communications ASAP Cartridges	Web Service (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High
CVE-2019-0222	Oracle Communications Diameter Signaling Router (DSR)	IDIH Visualization (Apache ActiveMQ)	HTTP	Yes	7.5	Network	Low
CVE-2017-12626	Oracle Communications Diameter Signaling Router (DSR)	IDIH Visualization (Apache POI)	HTTP	Yes	7.5	Network	Low
CVE-2018-15756	Oracle Communications Diameter Signaling Router (DSR)	IDIH Visualization (Spring Framework)	HTTP	Yes	7.5	Network	Low
CVE-2018-1000180	Oracle Communications Diameter Signaling Router (DSR)	IDIH Visualization (Bouncy Castle Java Library)	TLS	Yes	7.5	Network	Low
CVE-2019-0227	Oracle Communications Element Manager	Core (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERS		
					Base Score	Attack Vector	Attac Compl
CVE-2019-10072	Oracle Communications Element Manager	Core (Apache Tomcat)	HTTP	Yes	7.5	Network	Low
CVE-2019-15163	Oracle Communications Operations Monitor	Packet Inspector, Traces functionality (libpcap)	HTTP	Yes	7.5	Network	Low
CVE-2019-0227	Oracle Communications Session Report Manager	Core (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High
CVE-2019-10072	Oracle Communications Session Report Manager	Core (Apache Tomcat)	HTTP	Yes	7.5	Network	Low
CVE-2018-15756	Oracle Communications Session Report Manager	Core (Spring Framework)	HTTP	Yes	7.5	Network	Low
CVE-2019-0227	Oracle Communications Session Route Manager	Core (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High
CVE-2019-10072	Oracle Communications Session Route Manager	Core (Apache Tomcat)	HTTP	Yes	7.5	Network	Low
CVE-2018-15756	Oracle Communications Session Route Manager	Core (Spring Framework)	HTTP	Yes	7.5	Network	Low
CVE-2017-12626	Oracle Communications Unified Inventory Management	Bulk Import (Apache POI)	HTTP	Yes	7.5	Network	Low
CVE-2019-11358	Oracle Communications	IDIH Visualization	HTTP	Yes	6.1	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERS		
					Base Score	Attack Vector	Attac Compl
	Diameter Signaling Router (DSR)	(jQuery)					
CVE-2019-11358	Oracle Communications Operations Monitor	Mediation Engine, Calls Page (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2019-11358	Oracle Communications WebRTC Session Controller	WSC-Console (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2019-10247	Oracle Communications Element Manager	Core (Eclipse Jetty)	HTTP	Yes	5.3	Network	Low
CVE-2018-20852	Oracle Communications Operations Monitor	VSP Webserver (Python)	HTTP	Yes	5.3	Network	Low
CVE-2019-10247	Oracle Communications Session Report Manager	Core (Eclipse Jetty)	HTTP	Yes	5.3	Network	Low
CVE-2019-10247	Oracle Communications Session Route Manager	Core (Eclipse Jetty)	HTTP	Yes	5.3	Network	Low
CVE-2019-14821	Oracle SD-WAN Edge	OS (Kernel)	None	No	3.9	Local	High
CVE-2019-1010238	Oracle SD-WAN Edge	OS (Kernel)	SSH	No	2.0	Network	High

Notes:

1. Versions 7.3, 8.0 and 8.1 are vulnerable only with Debian 5.1. Version 8.2 is vulnerable only with Oracle Linux 7.0.

Additional CVEs addressed are below:

- The patch for CVE-2018-1000180 also addresses CVE-2018-1000613.
- The patch for CVE-2019-0211 also addresses CVE-2019-0196, CVE-2019-0197, CVE-2019-0215, CVE-2019-0217 and CVE-2019-0220.

- The patch for CVE-2019-0222 also addresses CVE-2018-11775.
- The patch for CVE-2019-0227 also addresses CVE-2018-8032.
- The patch for CVE-2019-10072 also addresses CVE-2018-11784.
- The patch for CVE-2019-10082 also addresses CVE-2019-10081, CVE-2019-10092, CVE-2019-10097, CVE-2019-10098 and CVE-2019-9517.
- The patch for CVE-2019-10088 also addresses CVE-2019-10093 and CVE-2019-10094.
- The patch for CVE-2019-10247 also addresses CVE-2019-10246.
- The patch for CVE-2019-14379 also addresses CVE-2019-14439.
- The patch for CVE-2019-15163 also addresses CVE-2019-15161, CVE-2019-15162, CVE-2019-15164 and CVE-2019-15165.
- The patch for CVE-2019-16943 also addresses CVE-2019-16942 and CVE-2019-17531.
- The patch for CVE-2019-2729 also addresses CVE-2019-2725.
- The patch for CVE-2019-5482 also addresses CVE-2019-15601 and CVE-2019-5481.

Oracle Construction and Engineering Risk Matrix

This Critical Patch Update contains 12 new security patches for Oracle Construction and Engineering. 9 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2017-5645	Instantis EnterpriseTrack	Logging (Log4j)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-17195	Primavera Gateway	Admin (Connect2id Nimbus JOSE+JWT)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-16943	Primavera Gateway	Admin (jackson-databind)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-16943	Primavera Unifier	Infrastructure (jackson-databind)	HTTP	Yes	9.8	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2019-13990	Primavera Unifier	Infrastructure (Quartz)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-10082	Instantis EnterpriseTrack	Generic (Apache HTTP Server)	HTTP	Yes	9.1	Network	Low	N
CVE-2019-17563	Instantis EnterpriseTrack	Generic (Apache Tomcat)	HTTP	Yes	7.5	Network	High	N
CVE-2019-12402	Primavera Gateway	Admin (Apache Commons Compress)	HTTP	Yes	7.5	Network	Low	N
CVE-2019-10086	Primavera Gateway	Admin (Apache Commons Beanutils)	HTTP	Yes	7.3	Network	Low	N
CVE-2020-2594	Primavera P6 Enterprise Project Portfolio Management	Project Manager	HTTP	No	6.5	Network	Low	
CVE-2019-12415	Instantis EnterpriseTrack	Office Open document processor (Apache POI)	None	No	5.5	Local	Low	
CVE-2020-2706	Primavera P6 Enterprise Project Portfolio Management	Project Manager	HTTP	No	5.4	Network	Low	

Additional CVEs addressed are below:

- The patch for CVE-2019-10082 also addresses CVE-2019-10081, CVE-2019-10092, CVE-2019-10097, CVE-2019-10098 and CVE-2019-9517.
- The patch for CVE-2019-13990 also addresses CVE-2019-5427.
- The patch for CVE-2019-16943 also addresses CVE-2019-16942 and CVE-2019-17531.

Oracle E-Business Suite Risk Matrix

This Critical Patch Update contains 74 new security patches for the Oracle E-Business Suite. 70 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

Oracle E-Business Suite products include Oracle Database and Oracle Fusion Middleware components that are affected by the vulnerabilities listed in the Oracle Database and Oracle Fusion Middleware sections. The exposure of Oracle E-Business Suite products is dependent on the Oracle Database and Oracle Fusion Middleware versions being used. Oracle Database and Oracle Fusion Middleware security updates are not listed in the Oracle E-Business Suite risk matrix. However, since vulnerabilities affecting Oracle Database and Oracle Fusion Middleware versions may affect Oracle E-Business Suite products, Oracle recommends that customers apply the April 2020 Critical Patch Update to the Oracle Database and Oracle Fusion Middleware components of Oracle E-Business Suite. For information on what patches need to be applied to your environments, refer to Oracle E-Business Suite Release 12 Critical Patch Update Knowledge Document (April 2020), My Oracle Support Note 2650675.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2020-2838	Oracle CRM Gateway for Mobile Devices	Setup of Mobile Applications	HTTP	Yes	8.6	Network	Low	No
CVE-2020-2863	Oracle Advanced Outbound Telephony	User Interface	HTTP	No	8.5	Network	Low	Lo
CVE-2020-2852	Oracle Advanced Outbound Telephony	Calendar	HTTP	Yes	8.2	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2020-2871	Oracle Advanced Outbound Telephony	User Interface	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2854	Oracle Advanced Outbound Telephony	User Interface	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2856	Oracle Advanced Outbound Telephony	User Interface	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2857	Oracle Advanced Outbound Telephony	User Interface	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2890	Oracle Applications Framework	Diagnostics	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2820	Oracle Common Applications Calendar	Notes	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2823	Oracle Common Applications Calendar	Notes	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2881	Oracle CRM Technical Foundation	Preferences	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2873	Oracle Customer Interaction History	Outcome-Result	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2842	Oracle Depot Repair	Estimate and Actual Charges	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2844	Oracle Depot Repair	Estimate and Actual Charges	HTTP	Yes	8.2	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2020-2845	Oracle Depot Repair	Estimate and Actual Charges	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2846	Oracle Depot Repair	Estimate and Actual Charges	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2847	Oracle Depot Repair	Estimate and Actual Charges	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2848	Oracle Depot Repair	Estimate and Actual Charges	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2849	Oracle Depot Repair	Estimate and Actual Charges	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2850	Oracle Depot Repair	Estimate and Actual Charges	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2885	Oracle Document Management and Collaboration	Attachments	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2808	Oracle E-Business Intelligence	DBI Setups	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2809	Oracle E-Business Intelligence	DBI Setups	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2840	Oracle E-Business Intelligence	DBI Setups	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2874	Oracle Email Center	Customer Search	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2794	Oracle Email Center	Email Address list and Message Display	HTTP	Yes	8.2	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.(			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2020-2813	Oracle Email Center	KB Search	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2796	Oracle Email Center	Message Display	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2855	Oracle iSupport	Admin	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2878	Oracle iSupport	Mail	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2843	Oracle iSupport	Profile	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2815	Oracle iSupport	Profile	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2872	Oracle iSupport	Profile	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2841	Oracle Knowledge Management	Setup, Admin	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2880	Oracle Learning Management	OTA Training Activities	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2831	Oracle Marketing	Marketing Administration	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2834	Oracle Marketing	Marketing Administration	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2835	Oracle Marketing	Marketing Administration	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2836	Oracle Marketing	Marketing Administration	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2837	Oracle Marketing	Marketing Administration	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2858	Oracle Marketing	Marketing Administration	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2860	Oracle Marketing	Marketing Administration	HTTP	Yes	8.2	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.(			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2020-2861	Oracle Marketing	Marketing Administration	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2876	Oracle Marketing	Marketing Administration	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2807	Oracle Marketing Encyclopedia System	Administration	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2824	Oracle One-to-One Fulfillment	Print Server	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2825	Oracle One-to-One Fulfillment	Print Server	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2826	Oracle One-to-One Fulfillment	Print Server	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2827	Oracle One-to-One Fulfillment	Print Server	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2832	Oracle One-to-One Fulfillment	Print Server	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2870	Oracle One-to-One Fulfillment	Print Server	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2877	Oracle Partner Management	Attribute Admin Setup	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2833	Oracle Quoting	Courseware	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2817	Oracle Scripting	Miscellaneous	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2879	Oracle Scripting	Miscellaneous	HTTP	Yes	8.2	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2020-2839	Oracle Service Intelligence	Internal Operations-Search	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2821	Oracle Trade Management	Budget	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2822	Oracle Trade Management	Claims	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2818	Oracle Universal Work Queue	Work Provider Administration	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2819	Oracle Universal Work Queue	Work Provider Administration	HTTP	Yes	8.2	Network	Low	No
CVE-2020-2882	Oracle Human Resources	Hierarchy Diagrammers	HTTP	No	8.1	Network	Low	Lo
CVE-2020-2956	Oracle Human Resources	Hierarchy Diagrammers	HTTP	No	8.1	Network	Low	Lo
CVE-2020-2750	Oracle General Ledger	Account Hierarchy Manager	HTTP	Yes	7.5	Network	Low	No
CVE-2020-2866	Oracle Applications Framework	Attachments / File Upload	HTTP	Yes	5.3	Network	Low	No
CVE-2020-2889	Oracle CRM Technical Foundation	Preferences	HTTP	Yes	5.3	Network	Low	No
CVE-2020-2887	Oracle Customer Interaction History	Outcome-Result	HTTP	Yes	5.3	Network	Low	No
CVE-2020-2864	Oracle iSupplier Portal	Accounts	HTTP	Yes	5.3	Network	Low	No
CVE-2020-2888	Oracle Marketing	Partners	HTTP	Yes	5.3	Network	Low	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.(			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2020-2753	Oracle Workflow	Workflow Notification Mailer	HTTP	Yes	5.3	Network	Low	No
CVE-2020-2886	Oracle CRM Technical Foundation	Preferences	HTTP	Yes	4.7	Network	Low	No
CVE-2020-2810	Oracle iStore	Shopping Cart	HTTP	Yes	4.7	Network	Low	No
CVE-2020-2789	Oracle iSupport	User Interface	HTTP	Yes	4.7	Network	Low	No
CVE-2020-2862	Oracle One-to-One Fulfillment	Print Server	HTTP	Yes	4.7	Network	Low	No
CVE-2020-2772	Oracle Human Resources	Absence Recording, Maintenance	HTTP	No	4.1	Network	Low	Lo

Oracle Enterprise Manager Risk Matrix

This Critical Patch Update contains 7 new security patches for Oracle Enterprise Manager. 5 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. None of these patches are applicable to client-only installations, i.e., installations that do not have Oracle Enterprise Manager installed. The English text form of this Risk Matrix can be found here.

Oracle Enterprise Manager products include Oracle Database and Oracle Fusion Middleware components that are affected by the vulnerabilities listed in the Oracle Database and Oracle Fusion Middleware sections. The exposure of Oracle Enterprise Manager products is dependent on the Oracle Database and Oracle Fusion Middleware versions being used. Oracle Database and Oracle Fusion Middleware security updates are not listed in the Oracle Enterprise Manager risk matrix. However, since vulnerabilities affecting Oracle Database and Oracle Fusion Middleware versions may affect Oracle Enterprise Manager products, Oracle recommends that customers apply the April 2020 Critical Patch Update to the Oracle Database and Oracle Fusion Middleware components of Enterprise Manager. For information on what patches need to be applied to your environments, refer to Critical Patch Update April 2020 Patch Availability Document for Oracle Products, My Oracle Support Note 2633852.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-2961	Enterprise Manager Base Platform	Discovery Framework (Oracle OHS)	HTTP	Yes	9.8	Network	Low	None
CVE-2018-11058	Oracle Real User Experience Insight	Processing (Oracle Instant Client)	Multiple	No	8.8	Network	Low	Low
CVE-2018-18311	Enterprise Manager Base Platform	Install (Perl)	HTTP	Yes	8.1	Network	High	None
CVE-2019-0227	Oracle Application Testing Suite	Oracle Flow Builder (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High	None
CVE-2019-1543	Enterprise Manager Base Platform	Discovery Framework (OpenSSL)	HTTPS	Yes	7.4	Network	High	None
CVE-2019-11358	Application Service Level Management	Service Level Agreements (jQuery)	HTTP	Yes	6.1	Network	Low	None
CVE-2020-2946	Application Performance Management	EM Request Monitoring	HTTP	No	6.0	Network	Low	High

Additional CVEs addressed are below:

- The patch for CVE-2018-11058 also addresses CVE-2016-0701, CVE-2016-2183, CVE-2016-6306, CVE-2016-8610, CVE-2018-11054, CVE-2018-11055, CVE-2018-11056, CVE-2018-11057 and CVE-2018-15769.
- The patch for CVE-2018-18311 also addresses CVE-2016-2381.
- The patch for CVE-2019-0227 also addresses CVE-2018-8032.

Oracle Financial Services Applications Risk Matrix

This Critical Patch Update contains 35 new security patches for Oracle Financial Services Applications. 16 of these vulnerabilities may be remotely exploitable without authentication,

i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2019-2904	Oracle Banking Enterprise Collections	Framework (Application Development Framework)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-13990	Oracle Banking Enterprise Originations	Core (Quartz)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-2904	Oracle Banking Enterprise Originations	Framework (Application Development Framework)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-13990	Oracle Banking Enterprise Product Manufacturing	Core (Quartz)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-2904	Oracle Banking Enterprise Product Manufacturing	Framework (Application Development Framework)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-2904	Oracle Banking Platform	Framework (Application Development Framework)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-16943	Oracle Banking Platform	Framework (jackson-databind)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-2904	Oracle Financial Services Revenue Management	Dashboards (Application Development Framework)	HTTP	Yes	9.8	Network	Low	N

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
	and Billing Analytics							
CVE-2019-12419	Oracle FLEXCUBE Private Banking	Core (Apache CXF)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-2904	Oracle FLEXCUBE Private Banking	Framework (Application Development Framework)	HTTP	Yes	9.8	Network	Low	N
CVE-2019-10088	Oracle FLEXCUBE Private Banking	Core (Apache Tika)	HTTP	Yes	8.8	Network	Low	N
CVE-2019-17359	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure (Bouncy Castle Java Library)	HTTP	Yes	7.5	Network	Low	N
CVE-2019-0227	Oracle FLEXCUBE Private Banking	Core (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High	N
CVE-2017-12626	Oracle FLEXCUBE Private Banking	Core (Apache POI)	HTTP	Yes	7.5	Network	Low	N
CVE-2020-2793	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure	HTTP	No	7.1	Network	Low	L
CVE-2020-2939	Oracle Financial Services Asset Liability Management	User Interface	HTTP	No	7.1	Network	Low	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2020-2936	Oracle Financial Services Balance Sheet Planning	User Interface	HTTP	No	7.1	Network	Low	L
CVE-2020-2964	Oracle Financial Services Data Foundation	User Interface	HTTP	No	7.1	Network	Low	L
CVE-2020-2945	Oracle Financial Services Deposit Insurance Calculations for Liquidity Risk Management	User Interfaces	HTTP	No	7.1	Network	Low	L
CVE-2020-2941	Oracle Financial Services Funds Transfer Pricing	User Interface	HTTP	No	7.1	Network	Low	L
CVE-2020-2935	Oracle Financial Services Hedge Management and IFRS Valuations	User Interface	HTTP	No	7.1	Network	Low	L
CVE-2020-2891	Oracle Financial Services Liquidity Risk Management	User Interfaces	HTTP	No	7.1	Network	Low	L
CVE-2020-2943	Oracle Financial Services Liquidity Risk Measurement	User Interface	HTTP	No	7.1	Network	Low	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
	and Management							
CVE-2020-2938	Oracle Financial Services Loan Loss Forecasting and Provisioning	User Interface	HTTP	No	7.1	Network	Low	L
CVE-2020-2942	Oracle Financial Services Price Creation and Discovery	User Interface	HTTP	No	7.1	Network	Low	L
CVE-2020-2940	Oracle Financial Services Profitability Management	User Interface	HTTP	No	7.1	Network	Low	L
CVE-2020-2937	Oracle Insurance Accounting Analyzer	User Interface	HTTP	No	7.1	Network	Low	L
CVE-2020-2955	Oracle FLEXCUBE Core Banking	Transaction Processing	HTTP	No	6.3	Network	Low	L
CVE-2019-17091	Oracle Banking Enterprise Product Manufacturing	Core (Eclipse Mojarra)	HTTP	Yes	6.1	Network	Low	N
CVE-2019-12415	Oracle Banking Enterprise Originations	Core (Apache POI)	None	No	5.5	Local	Low	L
CVE-2019-12415	Oracle Banking Enterprise Product Manufacturing	Core (Apache POI)	None	No	5.5	Local	Low	L

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3			
					Base Score	Attack Vector	Attack Complex	P R
CVE-2019-12415	Oracle Banking Platform	Core (Apache POI)	None	No	5.5	Local	Low	L
CVE-2019-12415	Oracle Financial Services Analytical Applications Infrastructure	Infrastructure (Apache POI)	None	No	5.5	Local	Low	L
CVE-2019-12415	Oracle Financial Services Market Risk Measurement and Management	Infrastructure (Apache POI)	None	No	5.5	Local	Low	L
CVE-2019-10247	Oracle FLEXCUBE Private Banking	Core (Eclipse Jetty)	HTTP	Yes	5.3	Network	Low	N

Additional CVEs addressed are below:

- The patch for CVE-2019-0227 also addresses CVE-2018-8032.
- The patch for CVE-2019-10088 also addresses CVE-2019-10093 and CVE-2019-10094.
- The patch for CVE-2019-10247 also addresses CVE-2019-10246.
- The patch for CVE-2019-12415 also addresses CVE-2017-12626.
- The patch for CVE-2019-12419 also addresses CVE-2019-12406.
- The patch for CVE-2019-13990 also addresses CVE-2019-5427.
- The patch for CVE-2019-16943 also addresses CVE-2019-16942 and CVE-2019-17531.

Oracle Food and Beverage Applications Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle Food and Beverage Applications. This vulnerability is not remotely exploitable without authentication, i.e., may not be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK (				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
CVE-2020-2746	Oracle Hospitality Reporting and Analytics	Admin	HTTP	No	8.1	Network	Low	Low	N

Oracle Fusion Middleware Risk Matrix

This Critical Patch Update contains 52 new security patches for Oracle Fusion Middleware. 45 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

Oracle Fusion Middleware products include Oracle Database components that are affected by the vulnerabilities listed in the Oracle Database section. The exposure of Oracle Fusion Middleware products is dependent on the Oracle Database version being used. Oracle Database security updates are not listed in the Oracle Fusion Middleware risk matrix. However, since vulnerabilities affecting Oracle Database versions may affect Oracle Fusion Middleware products, Oracle recommends that customers apply the Critical Patch Update April 2020 to the Oracle Database components of Oracle Fusion Middleware products. For information on what patches need to be applied to your environments, refer to Critical Patch Update April 2020 Patch Availability Document for Oracle Products, My Oracle Support Note 2633852.1.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION			
					Base Score	Attack Vector	Attack Complex	
CVE-2020-2950	Oracle Business Intelligence Enterprise Edition	Analytics Web General	HTTP	Yes	9.8	Network	Low	
CVE-2016-1000031	Oracle Business Intelligence Enterprise Edition	BI Platform Security (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	
CVE-2020-2915	Oracle Coherence	Caching, CacheStore, Invocation	IIOP, T3	Yes	9.8	Network	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2019-13990	Oracle Fusion Middleware MapViewer	Install (Quartz)	HTTP	Yes	9.8	Network	Low
CVE-2019-16943	Oracle Global Lifecycle Management NextGen OUI Framework	Tools (jackson-databind)	HTTP	Yes	9.8	Network	Low
CVE-2016-10328	Oracle Outside In Technology	Installation (FreeType)	HTTP	Yes	9.8	Network	Low
CVE-2019-16943	Oracle WebCenter Portal	Security Framework (jackson-databind)	HTTP	Yes	9.8	Network	Low
CVE-2019-16943	Oracle WebCenter Sites	Sites (jackson-databind)	HTTP	Yes	9.8	Network	Low
CVE-2019-17571	Oracle WebLogic Server	Console (Apache Log4j)	HTTP	Yes	9.8	Network	Low
CVE-2019-16943	Oracle WebLogic Server	Third Party Tools (jackson-databind)	HTTP	Yes	9.8	Network	Low
CVE-2020-2801	Oracle WebLogic Server	Core	IIOP, T3	Yes	9.8	Network	Low
CVE-2020-2883	Oracle WebLogic Server	Core	IIOP, T3	Yes	9.8	Network	Low
CVE-2020-2884	Oracle WebLogic Server	Core	IIOP, T3	Yes	9.8	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2019-10088	Oracle Business Process Management Suite	BPM Composer (Apache Tika)	HTTP	Yes	8.8	Network	Low
CVE-2017-5130	Oracle HTTP Server	Web Listener (LibXML2)	HTTP	Yes	8.8	Network	Low
CVE-2020-2867	Oracle WebLogic Server	Web Container	HTTP	Yes	8.2	Network	Low
CVE-2019-0222	Identity Manager Connector	General (Apache ActiveMQ)	HTTP	Yes	7.5	Network	Low
CVE-2018-15756	Identity Manager Connector	LDAP Gateway (Spring Framework)	HTTP	Yes	7.5	Network	Low
CVE-2015-7940	Oracle Business Intelligence Enterprise Edition	Installation (Bouncy Castle Java Library)	HTTPS	Yes	7.5	Network	Low
CVE-2017-12626	Oracle Endeca Information Discovery Integrator	Integrator ETL (Apache POI)	HTTP	Yes	7.5	Network	Low
CVE-2019-17359	Oracle Managed File Transfer	MFT Runtime Server (Bouncy Castle Java Library)	HTTPS	Yes	7.5	Network	Low
CVE-2019-15903	Oracle Outside In Technology	DC-Specific Component (LibExpat)	HTTP	Yes	7.5	Network	Low
CVE-2019-16168	Oracle Outside In Technology	DC-Specific Component (SQLite)	HTTP	Yes	7.5	Network	Low
CVE-2018-20843	Oracle Outside In Technology	Installation (FreeType)	HTTP	Yes	7.5	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2019-17359	Oracle SOA Suite	Installation (Bouncy Castle Java Library)	HTTPS	Yes	7.5	Network	Low
CVE-2019-17359	Oracle WebCenter Portal	Security Framework (Bouncy Castle Java Library)	HTTPS	Yes	7.5	Network	Low
CVE-2020-2828	Oracle WebLogic Server	WLS Web Services	IIOP, T3	Yes	7.5	Network	Low
CVE-2020-2739	Oracle WebCenter Sites	Advanced UI	HTTP	Yes	7.4	Network	Low
CVE-2020-2784	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.3	Network	Low
CVE-2020-2785	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.3	Network	Low
CVE-2020-2786	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.3	Network	Low
CVE-2020-2787	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	7.3	Network	Low
CVE-2020-2798	Oracle WebLogic Server	WLS Web Services	IIOP, T3	No	7.2	Network	Low
CVE-2020-2952	Oracle HTTP Server	Web Listener	HTTP	Yes	6.5	Network	Low
CVE-2018-20622	Oracle Outside In Technology	Installation (JasPer)	HTTP	Yes	6.5	Network	Low
CVE-2019-11358	Oracle Big Data Discovery	Studio (jQuery)	HTTP	Yes	6.1	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2019-11358	Oracle Fusion Middleware MapViewer	Install (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2019-11358	Oracle WebCenter Sites	Advanced UI (jQuery)	HTTP	Yes	6.1	Network	Low
CVE-2020-2811	Oracle WebLogic Server	Console	HTTP	Yes	6.1	Network	Low
CVE-2019-12415	Oracle Big Data Discovery	Studio (Apache POI)	None	No	5.5	Local	Low
CVE-2020-2747	Oracle Access Manager	SSO Engine	HTTP	No	5.4	Network	Low
CVE-2020-2949	Oracle Coherence	Caching, CacheStore, Invocation	HTTP	Yes	5.3	Network	Low
CVE-2019-10247	Oracle Endeca Information Discovery Integrator	Integrator ETL (Eclipse Jetty)	HTTP	Yes	5.3	Network	Low
CVE-2020-2783	Oracle Outside In Technology	Outside In Filters	HTTP	Yes	5.3	Network	Low
CVE-2019-10247	Oracle Unified Directory	OpenDS SDK (Eclipse Jetty)	HTTP	Yes	5.3	Network	Low
CVE-2020-2766	Oracle WebLogic Server	Console	HTTP	Yes	5.3	Network	Low
CVE-2020-2829	Oracle WebLogic Server	Management Services	HTTP	No	4.9	Network	Low

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2019-1547	Oracle API Gateway	Oracle API Gateway (OpenSSL)	None	No	4.7	Local	High
CVE-2019-1547	Oracle Endeca Server	Product Code (OpenSSL)	None	No	4.7	Local	High
CVE-2020-2740	Oracle Access Manager	Authentication Engine	HTTP	No	4.6	Network	Low
CVE-2020-2745	Oracle Access Manager	Federation	HTTP	Yes	4.3	Network	Low
CVE-2020-2869	Oracle WebLogic Server	Console	HTTP	Yes	4.3	Network	Low

Notes:

1. Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower.

2. The patch for this issue will address the vulnerability only if the WLS instance is using JDK 1.7.0_191 or later, or JDK 1.8.0_181 or later.

Additional CVEs addressed are below:

- The patch for CVE-2016-10328 also addresses CVE-2016-10244, CVE-2017-7857, CVE-2017-7858, CVE-2017-7864, CVE-2017-8105, CVE-2017-8287 and CVE-2018-6942.
- The patch for CVE-2018-20622 also addresses CVE-2017-13745, CVE-2017-14232, CVE-2018-18873, CVE-2018-19139, CVE-2018-19539, CVE-2018-19540, CVE-2018-19541, CVE-2018-19542, CVE-2018-19543, CVE-2018-20570, CVE-2018-20584, CVE-2018-9055, CVE-2018-9154 and CVE-2018-9252.
- The patch for CVE-2019-0222 also addresses CVE-2018-11775.
- The patch for CVE-2019-10088 also addresses CVE-2019-10093 and CVE-2019-10094.
- The patch for CVE-2019-10247 also addresses CVE-2019-10246.
- The patch for CVE-2019-13990 also addresses CVE-2019-5427.
- The patch for CVE-2019-1547 also addresses CVE-2019-1549, CVE-2019-1552 and CVE-2019-1563.

- The patch for CVE-2019-16168 also addresses CVE-2018-20346, CVE-2018-20506 and CVE-2019-8457.
- The patch for CVE-2019-16943 also addresses CVE-2019-16942 and CVE-2019-17531.
- The patch for CVE-2019-17571 also addresses CVE-2017-5645.
- The patch for CVE-2020-2798 also addresses CVE-2020-2963.

Oracle GraalVM Risk Matrix

This Critical Patch Update contains 5 new security patches for Oracle GraalVM. 2 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RIS				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2019-15606	Oracle GraalVM Enterprise Edition	JavaScript (Node.js)	Multiple	Yes	9.8	Network	Low	None	
CVE-2020-2803	Oracle GraalVM Enterprise Edition	Java	Multiple	Yes	8.3	Network	High	None	F
CVE-2020-2802	Oracle GraalVM Enterprise Edition	GraalVM Compiler	Multiple	No	7.7	Network	Low	Low	
CVE-2020-2799	Oracle GraalVM Enterprise Edition	GraalVM Compiler	Multiple	No	6.3	Network	High	Low	
CVE-2020-2900	Oracle GraalVM Enterprise Edition	Tools	Multiple	No	3.7	Network	High	Low	F

Additional CVEs addressed are below:

- The patch for CVE-2019-15606 also addresses CVE-2019-15604 and CVE-2019-15605.

Oracle Health Sciences Applications Risk Matrix

This Critical Patch Update contains 2 new security patches for Oracle Health Sciences Applications. Both of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2019-17091	Oracle Health Sciences Information Manager	Policy Engine (Eclipse Mojarra)	HTTP	Yes	6.1	Network	Low	None
CVE-2019-17091	Oracle Healthcare Data Repository	Installation (Eclipse Mojarra)	HTTP	Yes	6.1	Network	Low	None

Oracle Hyperion Risk Matrix

This Critical Patch Update contains 3 new security patches for Oracle Hyperion. None of these vulnerabilities may be remotely exploitable without authentication, i.e., none may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 R			
					Base Score	Attack Vector	Attack Complex	Privs Req'
CVE-2020-2777	Hyperion Financial Management	Security	HTTP	No	4.2	Network	High	High
CVE-2019-2899	Hyperion Financial Management	Security (Application Development Framework)	HTTP	No	2.4	Network	Low	High
CVE-2020-2769	Hyperion Financial Reporting	Web Based Report Designer	HTTP	No	2.4	Network	Low	High

Oracle Java SE Risk Matrix

This Critical Patch Update contains 15 new security patches for Oracle Java SE. All of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-2803	Java SE, Java SE Embedded	Libraries	Multiple	Yes	8.3	Network	High	None
CVE-2020-2805	Java SE, Java SE Embedded	Libraries	Multiple	Yes	8.3	Network	High	None
CVE-2019-18197	Java SE	JavaFX (libxslt)	Multiple	Yes	8.1	Network	High	None
CVE-2020-2816	Java SE	JSSE	HTTPS	Yes	7.5	Network	Low	None
CVE-2020-2781	Java SE, Java SE Embedded	JSSE	HTTPS	Yes	5.3	Network	Low	None
CVE-2020-2830	Java SE, Java SE Embedded	Concurrency	Multiple	Yes	5.3	Network	Low	None
CVE-2020-2767	Java SE	JSSE	HTTPS	Yes	4.8	Network	High	None
CVE-2020-2800	Java SE, Java SE Embedded	Lightweight HTTP Server	Multiple	Yes	4.8	Network	High	None

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RI			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
CVE-2020-2778	Java SE	JSSE	HTTPS	Yes	3.7	Network	High	None
CVE-2020-2764	Java SE	Advanced Management Console	Multiple	Yes	3.7	Network	High	None
CVE-2020-2754	Java SE, Java SE Embedded	Scripting	Multiple	Yes	3.7	Network	High	None
CVE-2020-2755	Java SE, Java SE Embedded	Scripting	Multiple	Yes	3.7	Network	High	None
CVE-2020-2773	Java SE, Java SE Embedded	Security	Multiple	Yes	3.7	Network	High	None
CVE-2020-2756	Java SE, Java SE Embedded	Serialization	Multiple	Yes	3.7	Network	High	None
CVE-2020-2757	Java SE, Java SE Embedded	Serialization	Multiple	Yes	3.7	Network	High	None

Notes:

1. This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does

not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).

2. This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service.

3. Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service.

Oracle JD Edwards Risk Matrix

This Critical Patch Update contains 4 new security patches for Oracle JD Edwards. 2 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2020-2733	JD Edwards EnterpriseOne Tools	Monitoring and Diagnostics	HTTP	Yes	9.8	Network	Low	No
CVE-2018-11058	JD Edwards EnterpriseOne Tools	Enterprise Infrastructure Security (Oracle Security Service)	JDENET	Yes	9.8	Network	Low	No
CVE-2019-1547	JD Edwards EnterpriseOne Tools	Enterprise Infrastructure Security (OpenSSL)	None	No	4.7	Local	High	Lo
CVE-2019-1547	JD Edwards World Security	World Software Security (OpenSSL)	None	No	4.7	Local	High	Lo

Additional CVEs addressed are below:

- The patch for CVE-2018-11058 also addresses CVE-2016-0701, CVE-2016-2183, CVE-2016-6306, CVE-2016-8610, CVE-2018-11054, CVE-2018-11055, CVE-2018-11056, CVE-2018-11057 and CVE-2018-15769.

- The patch for CVE-2019-1547 also addresses CVE-2019-1549, CVE-2019-1552 and CVE-2019-1563.

Oracle Knowledge Risk Matrix

This Critical Patch Update contains 16 new security patches for Oracle Knowledge. 15 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2020-2791	Oracle Knowledge	Information Manager Console	HTTP	Yes	9.8	Network	Low	Non
CVE-2016-1000031	Oracle Knowledge	Information Manager Console, Web Applications - InfoCenter (Apache Commons FileUpload)	HTTP	Yes	9.8	Network	Low	Non
CVE-2020-2931	Oracle Knowledge	Web Applications - InfoCenter	HTTP	Yes	9.8	Network	Low	Non
CVE-2015-1832	Oracle Knowledge	Web Applications - InfoCenter (Apache Derby)	HTTP	Yes	9.1	Network	Low	Non
CVE-2019-0227	Oracle Knowledge	Information Manager Console (Apache Axis)	HTTP	Yes	8.1	Network	High	Non
CVE-2016-3092	Oracle Knowledge	Web Applications - InfoCenter (Apache Commons Fileupload)	HTTP	Yes	7.5	Network	Low	Non

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req'
CVE-2015-0254	Oracle Knowledge	Information Manager Console (Apache Standard Taglibs)	HTTP	Yes	7.3	Network	Low	Non
CVE-2018-17197	Oracle Knowledge	Information Manager Console (Apache Tika)	HTTP	Yes	6.5	Network	Low	Non
CVE-2020-2795	Oracle Knowledge	Information Manager Console	None	No	6.3	Local	High	High
CVE-2019-11358	Oracle Knowledge	Answer Flow (jQuery)	HTTP	Yes	6.1	Network	Low	Non
CVE-2015-9251	Oracle Knowledge	Information Manager Console, Web Applications - InfoCenter (jQuery)	HTTP	Yes	6.1	Network	Low	Non
CVE-2017-14735	Oracle Knowledge	Web Applications - InfoCenter (AntiSamy)	HTTP	Yes	6.1	Network	Low	Non
CVE-2020-2524	Oracle Knowledge	InQuira Search	HTTP	Yes	5.9	Network	High	Non
CVE-2020-2932	Oracle Knowledge	Information Manager Console	HTTP	Yes	5.9	Network	High	Non
CVE-2020-2553	Oracle Knowledge	Information Manager Console	HTTP	Yes	4.8	Network	High	Non
CVE-2020-2522	Oracle Knowledge	Information Manager Console	HTTP	Yes	4.3	Network	Low	Non

Oracle MySQL Risk Matrix

This Critical Patch Update contains 45 new security patches for Oracle MySQL. 9 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.(			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2019-5482	MySQL Server	Server: Compiling (cURL)	MySQL Protocol	Yes	9.8	Network	Low	No
CVE-2019-19646	MySQL Workbench	MySQL Workbench (SQLite)	MySQL Workbench	Yes	9.8	Network	Low	No
CVE-2019-14889	MySQL Workbench	MySQL Workbench (libssh)	MySQL Workbench	No	8.0	Network	Low	Lo
CVE-2019-17563	MySQL Enterprise Monitor	Service Manager (Apache Tomcat)	HTTPS	Yes	7.5	Network	High	No
CVE-2019-15601	MySQL Server	Server: Compiling (cURL)	MySQL Protocol	Yes	7.5	Network	Low	No
CVE-2019-15601	MySQL Workbench	MySQL Workbench (cURL)	MySQL Workbench	Yes	7.5	Network	Low	No
CVE-2020-2780	MySQL Server	Server: DML	MySQL Protocol	No	6.5	Network	Low	Lo
CVE-2020-2790	MySQL Server	Server: Pluggable Auth	MySQL Protocol	No	6.5	Network	Low	Lo
CVE-2020-2768	MySQL Cluster	Cluster: General	Multiple	No	6.3	Network	Low	Lo

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2020-2804	MySQL Server	Server: Memcached	Memcached Protocol	Yes	5.9	Network	High	No
CVE-2020-2760	MySQL Server	InnoDB	MySQL Protocol	No	5.5	Network	Low	Hi
CVE-2020-2752	MySQL Client	C API	MySQL Protocol	No	5.3	Network	High	Lo
CVE-2020-2806	MySQL Server	Server: Compiling	MySQL Protocol	No	5.3	Network	High	Lo
CVE-2020-2934	MySQL Connectors	Connector/J	MySQL Protocol	Yes	5.0	Network	High	No
CVE-2020-2762	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2020-2814	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2020-2893	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2020-2895	MySQL Server	InnoDB	MySQL Protocol	No	4.9	Network	Low	Hi

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2020-2898	MySQL Server	Server: Charsets	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2020-2903	MySQL Server	Server: Connection Handling	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2020-2896	MySQL Server	Server: Information Schema	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2020-2770	MySQL Server	Server: Logging	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2020-2765	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2020-2892	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2020-2897	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2020-2923	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2020-2924	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2020-2901	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2020-2928	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2020-2904	MySQL Server	Server: Optimizer	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2020-2925	MySQL Server	Server: PS	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2020-2759	MySQL Server	Server: Replication	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2020-2763	MySQL Server	Server: Replication	MySQL Protocol	No	4.9	Network	Low	Hi

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2020-2761	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2020-2774	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2020-2853	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2020-2779	MySQL Server	Server: Security: Privileges	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2020-2812	MySQL Server	Server: Stored Procedure	MySQL Protocol	No	4.9	Network	Low	Hi
CVE-2020-2875	MySQL Connectors	Connector/J	MySQL Protocol	Yes	4.7	Network	High	No
CVE-2019-1547	MySQL Server	Server: Packaging (OpenSSL)	MySQL Protocol	No	4.7	Local	High	Lo
CVE-2020-2926	MySQL Server	Server: Group Replication GCS	MySQL Protocol	No	4.4	Network	High	Hi
CVE-2020-2921	MySQL Server	Server: Group Replication Plugin	MySQL Protocol	No	4.4	Network	High	Hi
CVE-2020-2930	MySQL Server	Server: Parser	MySQL Protocol	No	4.4	Network	High	Hi
CVE-2020-2922	MySQL Client	C API	MySQL Protocol	Yes	3.7	Network	High	No

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Pri Re
CVE-2020-2933	MySQL Connectors	Connector/J	MySQL Protocol	No	2.2	Network	High	Hi

Additional CVEs addressed are below:

- The patch for CVE-2019-1547 also addresses CVE-2019-1549, CVE-2019-1552 and CVE-2019-1563.
- The patch for CVE-2019-19646 also addresses CVE-2019-19242, CVE-2019-19244, CVE-2019-19317, CVE-2019-19603, CVE-2019-19645, CVE-2019-19880, CVE-2019-19923, CVE-2019-19924, CVE-2019-19925, CVE-2019-19926, CVE-2019-19959 and CVE-2019-20218.
- The patch for CVE-2019-5482 also addresses CVE-2019-5481.

Oracle PeopleSoft Risk Matrix

This Critical Patch Update contains 14 new security patches for Oracle PeopleSoft. 10 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2020-2776	PeopleSoft Enterprise PeopleTools	Security	HTTP	Yes	8.6	Network	Low	Nor
CVE-2019-0227	PeopleSoft Enterprise PeopleTools	Tools Admin API (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High	Nor
CVE-2020-2859	PeopleSoft Enterprise PeopleTools	nVision	HTTP	Yes	7.5	Network	Low	Nor
CVE-2019-17359	PeopleSoft Enterprise PeopleTools	Security (Bouncy Castle Java Library)	HTTPS	Yes	7.5	Network	Low	Nor

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2020-2782	PeopleSoft Enterprise PeopleTools	Query	HTTP	Yes	7.1	Network	Low	Nor
CVE-2020-2906	PeopleSoft Enterprise SCM Purchasing	Supplier Change	HTTP	No	6.5	Network	Low	Lov
CVE-2020-2954	PeopleSoft Enterprise HRMS	Candidate Gateway	HTTP	Yes	6.1	Network	Low	Nor
CVE-2020-2868	PeopleSoft Enterprise PeopleTools	Diagnostic Framework	HTTP	Yes	6.1	Network	Low	Nor
CVE-2020-2751	PeopleSoft Enterprise PeopleTools	Portal	HTTP	Yes	6.1	Network	Low	Nor
CVE-2020-2797	PeopleSoft Enterprise PeopleTools	Process Scheduler	HTTP	Yes	6.1	Network	Low	Nor
CVE-2020-2775	PeopleSoft Enterprise PeopleTools	Portal	HTTP	Yes	5.3	Network	Low	Nor
CVE-2020-2912	PeopleSoft Enterprise CS Campus Community	Self-Service	HTTP	No	5.0	Network	Low	Lov
CVE-2020-2899	PeopleSoft Enterprise SCM Purchasing	Purchasing	HTTP	No	4.8	Network	Low	Hig
CVE-2020-2947	PeopleSoft Enterprise HCM Absence Management	Absence Management	HTTP	No	4.3	Network	Low	Lov

Oracle Retail Applications Risk Matrix

This Critical Patch Update contains 27 new security patches for Oracle Retail Applications. 17 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited

over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2017-5645	Oracle Retail Advanced Inventory Planning	AIP Dashboard (Apache Ant)	HTTP	Yes	9.8	Network	Low
CVE-2019-13990	Oracle Retail Back Office	Security (Apache Quartz)	HTTP	Yes	9.8	Network	Low
CVE-2019-13990	Oracle Retail Central Office	Security (Apache Quartz)	HTTP	Yes	9.8	Network	Low
CVE-2020-2953	Oracle Retail Customer Management and Segmentation Foundation	Promotions	HTTP	Yes	9.8	Network	Low
CVE-2019-13990	Oracle Retail Order Broker	Order Broker Foundation (Apache Quartz)	HTTP	Yes	9.8	Network	Low
CVE-2019-13990	Oracle Retail Point-of-Service	Security (Apache Quartz)	HTTP	Yes	9.8	Network	Low
CVE-2018-11058	Oracle Retail Predictive Application Server	RPAS Server (Oracle Security Service)	Multiple	Yes	9.8	Network	Low
CVE-2019-13990	Oracle Retail Returns Management	Security (Apache Quartz)	HTTP	Yes	9.8	Network	Low
CVE-2019-2880	Oracle Retail Store Inventory Management	Security	HTTP	No	8.8	Network	Low
CVE-2019-17563	MICROS Relate CRM Software	Segments (Apache Tomcat)	HTTP	Yes	7.5	Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
CVE-2019-17563	Oracle Retail Order Broker	System Administration (Apache Tomcat)	HTTP	Yes	7.5	Network	High
CVE-2020-5398	Oracle Retail Order Broker	System Administration (Spring Framework)	HTTP	Yes	7.5	Network	High
CVE-2017-5533	Oracle Retail Xstore Point of Service	Point of Sale (JasperReports)	HTTP	No	7.5	Network	High
CVE-2019-0227	Oracle Retail Xstore Point of Service	Xenvironment (Apache Axis)	HTTP	Yes	7.5	Adjacent Network	High
CVE-2019-17359	Oracle Retail Xstore Point of Service	Xenvironment (Bouncy Castle Java Library)	HTTPS	Yes	7.5	Network	Low
CVE-2017-12626	Oracle Retail Xstore Point of Service	Xenvironment (Apache POI)	HTTP	Yes	6.5	Network	Low
CVE-2019-17091	Oracle Retail Advanced Inventory Planning	AIP Dashboard (Eclipse Mojarra)	HTTP	Yes	6.1	Network	Low
CVE-2019-17091	Oracle Retail Merchandising System	Inventory Tracking (Eclipse Mojarra)	HTTP	Yes	6.1	Network	Low
CVE-2018-10237	Oracle Retail Xstore Point of Service	Xstore Office (Google Guava)	HTTP	Yes	5.9	Network	High
CVE-2017-3160	Oracle Retail Xstore Point of Service	Xstore Services (Apache Cordova)	None	No	4.2	Local	High
CVE-2019-10173	Oracle Retail Xstore Point of Service	Point of Sale (xstream)	HTTP	No	3.9	Network	High
CVE-2019-10086	Oracle Retail Xstore Point of	Xenvironment (Apache	HTTP	No	3.9	Network	High

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION		
					Base Score	Attack Vector	Attack Complex
	Service	Commons)					
CVE-2019-10072	Oracle Retail Xstore Point of Service	Xstore Services (Apache Tomcat)	HTTP	No	3.9	Network	High
CVE-2018-1258	Oracle Retail Xstore Point of Service	Xenvironment (jackson-databind)	HTTP	No	3.7	Network	High
CVE-2019-10082	Oracle Retail Xstore Point of Service	Xstore Office (Apache HTTP Server)	HTTP	No	3.3	Network	High
CVE-2018-11797	Oracle Retail Xstore Point of Service	Dataloader (Apache pdfbox)	HTTP	No	3.1	Network	High
CVE-2018-10237	Oracle Retail Xstore Point of Service	Xstore Services (Google Guava)	HTTP	No	3.1	Network	High

Additional CVEs addressed are below:

- The patch for CVE-2017-5533 also addresses CVE-2017-5529.
- The patch for CVE-2018-11058 also addresses CVE-2016-0701, CVE-2016-2183, CVE-2016-6306, CVE-2016-8610, CVE-2018-11054, CVE-2018-11055, CVE-2018-11056, CVE-2018-11057 and CVE-2018-15769.
- The patch for CVE-2018-11797 also addresses CVE-2018-8036 and CVE-2019-0228.
- The patch for CVE-2019-0227 also addresses CVE-2018-8032.
- The patch for CVE-2019-10072 also addresses CVE-2017-15706, CVE-2018-11784, CVE-2018-1304, CVE-2018-1305, CVE-2018-1336, CVE-2018-8014, CVE-2018-8034, CVE-2018-8037, CVE-2019-0199, CVE-2019-0221 and CVE-2019-0232.
- The patch for CVE-2019-10082 also addresses CVE-2019-10081, CVE-2019-10092, CVE-2019-10097, CVE-2019-10098 and CVE-2019-9517.
- The patch for CVE-2019-13990 also addresses CVE-2019-5427.
- The patch for CVE-2020-5398 also addresses CVE-2020-5397.

Oracle Siebel CRM Risk Matrix

This Critical Patch Update contains 1 new security patch for Oracle Siebel CRM. This vulnerability is not remotely exploitable without authentication, i.e., may not be exploited over a

network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2020-2738	Siebel UI Framework	EAI, SWSE	HTTP	No	4.3	Network	Low	Low	

Oracle Supply Chain Risk Matrix

This Critical Patch Update contains 4 new security patches for Oracle Supply Chain. 3 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0			
					Base Score	Attack Vector	Attack Complex	Priv Req
CVE-2017-5645	Oracle In-Memory Performance-Driven Planning	User Interface (Log4j)	HTTP	Yes	9.8	Network	Low	Non
CVE-2020-2920	Oracle Agile PLM	Security	HTTP	Yes	6.1	Network	Low	Non
CVE-2020-2744	Oracle Transportation Management	Security	HTTP	No	5.4	Network	Low	Lov
CVE-2020-2865	Oracle Configurator	Installation	HTTP	Yes	5.3	Network	Low	Non

Oracle Support Tools Risk Matrix

This Critical Patch Update contains 2 new security patches for Oracle Support Tools. Both of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK (				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	U Int
CVE-2019-5482	OSS Support Tools	Services Tools Bundle (cURL)	Multiple	Yes	9.8	Network	Low	None	N
CVE-2019-15601	OSS Support Tools	Services Tools Bundle (cURL)	Multiple	Yes	7.5	Network	Low	None	N

Additional CVEs addressed are below:

- The patch for CVE-2019-5482 also addresses CVE-2019-5435, CVE-2019-5436, CVE-2019-5443 and CVE-2019-5481.

Oracle Systems Risk Matrix

This Critical Patch Update contains 9 new security patches for Oracle Systems. 2 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RIS				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2019-2729	StorageTek Tape Analytics SW Tool	Application Server (Oracle WebLogic Server)	HTTP	Yes	9.8	Network	Low	None	
CVE-2020-2944	Oracle Solaris	Common Desktop Environment	None	No	8.8	Local	Low	Low	
CVE-2020-2927	Oracle Solaris	Common Desktop Environment	None	No	7.8	Local	High	Low	
CVE-2020-2851	Oracle Solaris	Common Desktop Environment	None	No	7.8	Local	High	Low	
CVE-2018-1165	Oracle Solaris	SMB Server Kernel	None	No	7.0	Local	High	Low	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RIS			
					Base Score	Attack Vector	Attack Complex	Privs Req'd
		Module						
CVE-2018-1165	Oracle ZFS Storage Appliance Kit	Operating System Image	Multiple	No	7.0	Local	High	Low
CVE-2019-11358	StorageTek Tape Analytics SW Tool	Software (jQuery)	HTTP	Yes	6.1	Network	Low	None
CVE-2020-2749	Oracle Solaris	SMF command svcbundle	None	No	2.5	Local	High	Low
CVE-2020-2771	Oracle Solaris	Whodo	None	No	2.5	Local	High	Low

Additional CVEs addressed are below:

- The patch for CVE-2018-1165 also addresses CVE-2016-6489, CVE-2017-5754, CVE-2018-0732, CVE-2018-0734, CVE-2018-0737, CVE-2018-18227, CVE-2018-19622, CVE-2018-19623, CVE-2018-19624, CVE-2018-19625, CVE-2018-19626, CVE-2018-19627, CVE-2018-19628, CVE-2018-5407, CVE-2019-12387, CVE-2019-12855, CVE-2019-13057, CVE-2019-13565, CVE-2019-16056, CVE-2019-16168, CVE-2019-19269, CVE-2019-19553, CVE-2019-2412, CVE-2019-2878, CVE-2019-3008, CVE-2019-9579, CVE-2020-2558, CVE-2020-2578, CVE-2020-2680, CVE-2020-2749 and CVE-2020-7044.
- The patch for CVE-2019-2729 also addresses CVE-2019-2725.

Oracle Utilities Applications Risk Matrix

This Critical Patch Update contains 2 new security patches for Oracle Utilities Applications. Both of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.(			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2018-1000632	Oracle Utilities Framework	Common (Dom4J)	HTTP	Yes	7.5	Network	Low	N(

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.(			
					Base Score	Attack Vector	Attack Complex	Pr Re
CVE-2017-12626	Oracle Utilities Network Management System	Upload (Apache POI)	HTTP	Yes	7.5	Network	Low	N(

Oracle Virtualization Risk Matrix

This Critical Patch Update contains 20 new security patches for Oracle Virtualization. 1 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2020-2902	Oracle VM VirtualBox	Core	None	No	8.8	Local	Low	Low	
CVE-2020-2959	Oracle VM VirtualBox	Core	MLD	Yes	8.6	Network	Low	None	
CVE-2020-2742	Oracle VM VirtualBox	Core	None	No	8.2	Local	Low	High	
CVE-2020-2905	Oracle VM VirtualBox	Core	None	No	8.2	Local	Low	High	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2020-2908	Oracle VM VirtualBox	Core	None	No	8.2	Local	Low	High	
CVE-2020-2758	Oracle VM VirtualBox	Core	None	No	8.2	Local	Low	High	
CVE-2020-2929	Oracle VM VirtualBox	Core	None	No	7.8	Local	Low	Low	
CVE-2020-2575	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High	
CVE-2020-2911	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High	
CVE-2020-2907	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High	
CVE-2020-2958	Oracle VM VirtualBox	Core	None	No	7.5	Local	High	High	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2020-2913	Oracle VM VirtualBox	Core	None	No	7.0	Local	High	Low	
CVE-2020-2914	Oracle VM VirtualBox	Core	None	No	7.0	Local	High	Low	
CVE-2020-2910	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	
CVE-2020-2951	Oracle VM VirtualBox	Core	None	No	6.5	Local	Low	Low	
CVE-2020-2741	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	
CVE-2020-2743	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	
CVE-2020-2894	Oracle VM VirtualBox	Core	None	No	6.0	Local	Low	High	
CVE-2020-2748	Oracle VM VirtualBox	Core	None	No	3.2	Local	Low	High	

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	I
CVE-2020-2909	Oracle VM VirtualBox	Core	None	No	2.8	Local	Low	Low	R