TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
04/16/2019

SUBJECT:
Oracle Quarterly Critical Patches Issued April 16, 2019

OVERVIEW:
Multiple vulnerabilities have been discovered in Oracle products, which could allow for remote code execution.

SYSTEMS AFFECTED:

- Agile Recipe Management for Pharmaceuticals, versions 9.3.3, 9.3.4
- Enterprise Manager Base Platform, versions 12.1.0.5.0, 13.2.0.0.0, 13.3.0.0.0
- Enterprise Manager Ops Center, version 12.3.3
- FMW Platform, version 12.2.1.3.0
- Instantis EnterpriseTrack, versions 17.1, 17.2, 17.3
- JD Edwards EnterpriseOne Tools, version 9.2
- JD Edwards World Technical Foundation, versions A9.2, A9.3.1, A9.4
- MICROS Lucas, versions 2.9.5.6, 2.9.5.7
- MICROS Relate CRM Software, version 11.4
- MICROS Retail-J, version 12.1.2
- MySQL Connectors, versions 5.3.12 and prior, 8.0.15 and prior
- MySQL Enterprise Backup, versions 3.12.3 and prior, 4.1.2 and prior
- MySQL Enterprise Monitor, versions 4.0.8 and prior, 8.0.14 and prior
- MySQL Server, versions 5.6.43 and prior, 5.7.25 and prior, 8.0.15 and prior
- Oracle Agile PLM, versions 9.3.3, 9.3.4, 9.3.5
- Oracle API Gateway, version 11.1.2.4.0
- Oracle Application Testing Suite, version 13.3.0.1
- Oracle AutoVue 3D Professional Advanced, versions 21.0.0, 21.0.1
- Oracle Banking Platform, versions 2.4.0, 2.4.1, 2.5.0, 2.6.0
- Oracle Berkeley DB, versions prior to 6.138, prior to 18.1.32
- Oracle BI Publisher, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0
- Oracle Business Intelligence Enterprise Edition, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0
- Oracle Business Process Management Suite, versions 11.1.1.9.0, 12.1.3.0.0, 12.2.1.3.0

- Oracle Business Transaction Management, version 12.1.0
- Oracle Commerce Merchandising, version 11.2.0.3
- Oracle Commerce Platform, versions 11.2.0.3, 11.3.1
- Oracle Communications Application Session Controller, versions 3.7.1, 3.8.0
- Oracle Communications EAGLE Application Processor, versions 16.1.0, 16.2.0
- Oracle Communications EAGLE LNP Application Processor, versions 10.0, 10.1, 10.2
- Oracle Communications Instant Messaging Server, version 10.0.1
- Oracle Communications Interactive Session Recorder, versions 6.0, 6.1, 6.2
- Oracle Communications LSMS, versions 13.1, 13.2, 13.3
- Oracle Communications Messaging Server, versions 8.0, 8.1
- Oracle Communications Operations Monitor, versions 3.4, 4.0
- Oracle Communications Policy Management, versions 12.1, 12.2, 12.3, 12.4
- Oracle Communications Pricing Design Center, versions 11.1, 12.0
- Oracle Communications Service Broker Engineered System Edition, version 6.0
- Oracle Communications Service Broker, version 6.0
- Oracle Communications Session Border Controller, versions 8.0.0, 8.1.0, 8.2.0
- Oracle Communications Unified Inventory Management, versions 7.3.2, 7.3.4, 7.3.5, 7.4.0
- Oracle Configuration Manager, version 12.1.0
- Oracle Configurator, versions 12.1, 12.2
- Oracle Data Integrator, versions 11.1.1.9.0, 12.2.1.3.0
- Oracle Database Server, versions 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c, 19c
- Oracle E-Business Suite, versions 0.9.8, 1.0.0, 1.0.1, 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7, 12.2.8
- Oracle Endeca Information Discovery Integrator, version 3.2.0
- Oracle Enterprise Communications Broker, versions 3.0.0, 3.1.0
- Oracle Enterprise Operations Monitor, versions 3.4, 4.0
- Oracle Enterprise Session Border Controller, versions 8.0.0, 8.1.0, 8.2.0
- Oracle Financial Services Analytical Applications Infrastructure, versions 7.3.3 - 7.3.5, 8.0.0 - 8.0.7
- Oracle Financial Services Asset Liability Management, versions 8.0.4 - 8.0.7
- Oracle Financial Services Data Integration Hub, versions 8.0.5 - 8.0.7
- Oracle Financial Services Funds Transfer Pricing, versions 8.0.4 - 8.0.7
- Oracle Financial Services Hedge Management and IFRS Valuations, versions 8.0.4 - 8.0.7
- Oracle Financial Services Liquidity Risk Management, versions 8.0.2 - 8.0.6
- Oracle Financial Services Loan Loss Forecasting and Provisioning, versions 8.0.2 - 8.0.7
- Oracle Financial Services Market Risk Measurement and Management, versions 8.0.5, 8.0.6
- Oracle Financial Services Profitability Management, versions 8.0.4 - 8.0.6
- Oracle Financial Services Reconciliation Framework, versions 8.0.5, 8.0.6
- Oracle FLEXCUBE Private Banking, versions 2.0.0.0, 2.2.0.1, 12.0.1.0, 12.0.3.0, 12.1.0.0
- Oracle Fusion Middleware MapViewer, version 12.2.1.3.0
- Oracle Health Sciences Data Management Workbench, version 2.4.8
- Oracle Healthcare Master Person Index, versions 3.0, 4.0

- Oracle Hospitality Cruise Dining Room Management, version 8.0.80
- Oracle Hospitality Cruise Fleet Management, version 9.0.11
- Oracle Hospitality Guest Access, versions 4.2.0, 4.2.1
- Oracle Hospitality Reporting and Analytics, version 9.1.0
- Oracle HTTP Server, version 12.2.1.3.0
- Oracle Identity Analytics, version 11.1.1.5.8
- Oracle Java SE Embedded, version 8u201
- Oracle Java SE, versions 7u211, 8u202, 11.0.2, 12
- Oracle JDeveloper, versions 11.1.1.9.0, 12.1.3.0.0, 12.2.1.3.0
- Oracle Knowledge, versions 8.5.1.0 - 8.5.1.7, 8.6.0, 8.6.1
- Oracle Managed File Transfer, versions 12.1.3.0.0, 12.2.1.3.0
- Oracle Outside In Technology, versions 8.5.3, 8.5.4
- Oracle Real-Time Scheduler, version 2.3.0
- Oracle Retail Allocation, version 15.0.2
- Oracle Retail Convenience Store Back Office, version 3.6
- Oracle Retail Customer Engagement, versions 16.0, 17.0
- Oracle Retail Customer Management and Segmentation Foundation, versions 16.0, 17.0, 18.0
- Oracle Retail Invoice Matching, versions 12.0, 13.0, 13.1, 13.2, 14.0, 14.1, 15.0
- Oracle Retail Merchandising System, versions 15.0, 16.0
- Oracle Retail Order Broker, versions 5.1, 5.2, 15.0, 16.0
- Oracle Retail Point-of-Service, versions 13.4, 14.0, 14.1
- Oracle Retail Workforce Management Software, version 1.60.9.0.0
- Oracle Retail Xstore Point of Service, versions 7.0, 7.1
- Oracle Secure Global Desktop, version 5.4
- Oracle Service Bus, versions 11.1.1.9.0, 12.1.3.0.0, 12.2.1.3.0
- Oracle SOA Suite, versions 11.1.1.9.0, 12.1.3.0.0, 12.2.1.3.0
- Oracle Solaris, versions 10, 11
- Oracle Traffic Director, version 11.1.1.9.0
- Oracle Transportation Management, versions 6.3.7, 6.4.2, 6.4.3
- Oracle Tuxedo, version 12.1.1.0.0
- Oracle Utilities Framework, versions 2.2.0, 4.2.0.2.0, 4.2.0.3.0, 4.3.0.2.0, 4.3.0.3.0, 4.3.0.4.0, 4.3.0.5.0, 4.3.0.6.0, 4.4.0.0.0, 4.4.0.1.0, 18.1.0.0.0, 18.2.0.0.0
- Oracle Utilities Mobile Workforce Management, version 2.3.0
- Oracle Utilities Network Management System, version 1.12.0.3
- Oracle VM VirtualBox, versions prior to 5.2.28, prior to 6.0.6
- Oracle WebCenter Portal, version 12.2.1.3.0
- Oracle WebCenter Sites, version 12.2.1.3.0
- Oracle WebLogic Server, versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0
- OSS Support Tools, version 19.1
- PeopleSoft Enterprise ELM Enterprise Learning Management, version 9.2
- PeopleSoft Enterprise ELM, version 9.2
- PeopleSoft Enterprise HCM Talent Acquisition Manager, version 9.2
- PeopleSoft Enterprise HRMS, version 9.2
- PeopleSoft Enterprise PeopleTools, versions 8.55, 8.56, 8.57
- PeopleSoft Enterprise PT PeopleTools, versions 8.55, 8.56, 8.57
- Primavera P6 Enterprise Project Portfolio Management, versions 8.4, 15.1, 15.2, 16.1, 16.2, 17.7 - 17.12, 18.8

- Primavera Unifier, versions 16.1, 16.2, 17.7 - 17.12, 18.8
- Siebel Applications, version 19.3

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Oracle to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Oracle:
https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html