

TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER: 2018-115

DATE(S) ISSUED: 10/16/2018

SUBJECT: Oracle Quarterly Critical Patches Issued October 16, 2018

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

SYSTEMS AFFECTED:

- Application Management Pack for Oracle E-Business Suite, versions 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7
- Enterprise Manager Base Platform, versions 12.1.0.5, 13.2.0.0
- Enterprise Manager for MySQL Database, versions 13.2.1.0.0, 13.2.2.0.0, 13.2.3.0.0
- Enterprise Manager Ops Center, versions 12.2.2, 12.3.3
- Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers, versions
- Prior to XCP2352 and Prior to XCP3050
- Hyperion BI+, version 11.1.2.4
- Hyperion Common Events, version 11.1.2.4
- Hyperion Data Relationship Management, version 11.1.2.4.345
- Hyperion Essbase Administration Services, version 11.1.2.4
- Instantis EnterpriseTrack, versions 17.1, 17.2, 17.3
- JD Edwards EnterpriseOne Orchestrator, version 9.2
- JD Edwards EnterpriseOne Tools, version 9.2
- MICROS Lucas, version 2.9.5
- MICROS PC Workstation 2015, versions Prior to BIOS 01.3.0.2i
- MICROS Relate CRM Software, versions 10.8, 11.4, 16.0, 17.0
- MICROS Retail-J, versions 12.1, 13.0
- MICROS XBRI, versions 10.5.0, 10.6.0, 10.7.0, 10.8.1, 10.8.2, 10.8.3
- MySQL Connectors, versions 8.0.12 and prior
- MySQL Enterprise Monitor, versions 3.4.9.4237 and prior, 4.0.6.5281 and prior, 8.0.2.8191 and prior
- MySQL Server, versions 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior, 8.0.12 and prior
- Oracle Adaptive Access Manager, versions 11.1.1.7.0, 11.1.2.3.0
- Oracle Agile Engineering Data Management, versions 6.1.3, 6.2.0, 6.2.1
- Oracle Agile PLM, versions 9.3.3, 9.3.4, 9.3.5, 9.3.6
- Oracle Agile PLM Framework, versions 9.3.3, 9.3.4, 9.3.5, 9.3.6
- Oracle Agile Product Lifecycle Management for Process, version 6.2.0.0
- Oracle API Gateway, version 11.1.2.4.0
- Oracle Banking Platform, versions 2.5.0, 2.6.0, 2.6.1, 2.6.2
- Oracle BI Publisher, versions 11.1.1.7.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0
- Oracle Big Data Discovery, version 1.6.0
- Oracle Business Intelligence Enterprise Edition, versions 11.1.1.7.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0
- Oracle Communications Application Session Controller, versions Prior to 3.7.1M0
- Oracle Communications Instant Messaging Server, versions prior to 10.0.1
- Oracle Communications Messaging Server, versions prior to 8.0.2
- Oracle Communications MetaSolv Solution, version 6.3.0
- Oracle Communications Performance Intelligence Center (PIC) Software, versions prior to 10.2.1
- Oracle Communications User Data Repository, versions prior to 12.2.0
- Oracle Configuration Manager, versions 12.1.2.0.2, 12.1.2.0.5
- Oracle Database Server, versions 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c
- Oracle Demantra Demand Management, versions 7.3.5, 12.2

- Oracle Directory Server Enterprise Edition, version 11.1.1.7
- Oracle E-Business Suite, versions 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7
- Oracle Endeca Information Discovery Integrator, versions 3.1.0, 3.2.0
- Oracle Endeca Information Discovery Studio, versions 3.1.0, 3.2.0
- Oracle Endeca Server, versions 6.7.1, 7.7.0
- Oracle Enterprise Repository, versions 11.1.1.7.0, 12.1.3.0.0
- Oracle GlassFish Server, version 3.1.2
- Oracle GoldenGate, versions 12.1.2.0.0, 12.1.2.1.0, 12.1.2.1.1, 12.2.0.1.0, 12.2.0.2.0, 12.3.0.1.0
- Oracle Healthcare Translational Research, version 3.1.0
- Oracle Hospitality Cruise Fleet Management, version 9.0
- Oracle Hospitality Cruise Shipboard Property Management System, version 8.0
- Oracle Hospitality Gift and Loyalty, version 9.0
- Oracle Hospitality Guest Access, versions 4.2.0, 4.2.1
- Oracle Hospitality Materials Control, version 18.1
- Oracle Hospitality Reporting and Analytics, version 9.0
- Oracle HTTP Server, version 12.2.1.3
- Oracle Identity Analytics, version 11.1.1.5.8
- Oracle Identity Management Suite, versions 11.1.2.3.0, 12.2.1.3.0
- Oracle Identity Manager, versions 11.1.2.3.0, 12.2.1.3.0
- Oracle iLearning, versions 6.1, 6.2
- Oracle Insurance Calculation Engine, versions 10.1.1, 10.2.1
- Oracle Insurance Rules Palette, versions 9.6, 9.7, 10.0, 10.1, 10.2, 11.0
- Oracle Java SE, versions 6u201, 7u191, 8u182, 11
- Oracle Java SE Embedded, version 8u181
- Oracle JRockit, version R28.3.19
- Oracle Outside In Technology, version 8.5.3
- Oracle Real-Time Decision Server, version 3.2.1
- Oracle Retail Allocation, versions 14.1, 15.0, 16.0
- Oracle Retail Assortment Planning, versions 14.1, 15.0, 16.0
- Oracle Retail Back Office, versions 13.3, 13.4, 14, 14.1
- Oracle Retail Brand Compliance Management, version 17.0.8.0
- Oracle Retail Central Office, version 14.1
- Oracle Retail Customer Engagement, version 16.0
- Oracle Retail Extract Transform and Load, versions 13.0, 13.1, 13.2
- Oracle Retail Financial Integration, versions 13.2, 14.0, 14.1, 15.0, 16.0
- Oracle Retail Integration Bus, version 14.1.2
- Oracle Retail Invoice Matching, versions 15.0, 16.0
- Oracle Retail Merchandising System, versions 15.0, 16.0
- Oracle Retail Open Commerce Platform, versions 5.3, 6.0, 6.0.1
- Oracle Retail Order Broker, versions 5.0, 5.1, 5.2, 15.0, 16.0
- Oracle Retail Point-of-Service, versions 13.4, 14.0, 14.1
- Oracle Retail Predictive Application Server, versions 14.0, 14.1, 15.0, 16.0
- Oracle Retail Returns Management, version 14.1
- Oracle Retail Sales Audit, versions 15.0, 16.0
- Oracle Retail Xstore Point of Service, versions 6.5, 7.0, 7.1, 15.0, 16.0, 17.0
- Oracle Service Bus, versions 12.1.3.0.0, 12.2.1.3.0
- Oracle Transportation Management, version 6.3.7
- Oracle Tuxedo, version 12.1.1.0
- Oracle Virtual Directory, versions 11.1.1.7.0, 11.1.1.9.0
- Oracle VM VirtualBox, versions prior to 5.2.20
- Oracle WebCenter Portal, versions 11.1.1.9.0, 12.2.1.3.0
- Oracle WebCenter Sites, versions 11.1.1.8.0, 12.2.1.3.0
- Oracle WebLogic Server, versions 10.3.6.0, 12.1.3.0, 12.2.1.3, Docker 12.2.1.3.20180913

- OSS Support Tools, versions prior to 18.4
- PeopleSoft Enterprise Interaction Hub, version 9.1.0.0
- PeopleSoft Enterprise PeopleTools, versions 8.55, 8.56, 8.57
- Primavera Gateway, versions 15.2, 16.2, 17.12
- Primavera P6 Enterprise Project Portfolio Management, versions 8.4, 15.1, 15.2, 16.1, 16.2, 18.8, 17.7 - 17.12
- Primavera Unifier, versions 15.1, 15.2, 16.1, 16.2, 17.1-17.12, 18.1-18.8
- Siebel Applications, versions 18.7, 18.8, 18.9
- Solaris, versions 10, 11.3, 11.4
- SPARC Enterprise M3000, M4000, M5000, M8000, M9000 Servers, versions prior to XCP 1123
- Spatial, versions 2.0, 2.1, 2.2

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:

We recommend the following actions 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/cpuoct2018-4428296.html>

24x7 Security Operations Center
 Multi-State Information Sharing and Analysis Center (MS-ISAC)
 Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
 31 Tech Valley Drive
 East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722



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/>