Alert – Oracle Quarterly Critical Patches issued - JULY 16, 2019

Description:

Oracle released critical patch updates for multiple vulnerabilities that have been discovered in Oracle products, which could allow for remote code execution. A remote attacker may cause the application to crash or execute arbitrary code by leveraging these vulnerabilities. Users of the affected products are recommended to update to the latest version appropriately

Vulnerable or affected systems:

- Application Express, versions 5.1, 18.2
- Diagnostic Assistant, versions prior to 2.12.36
- Enterprise Manager Base Platform, versions 12.1.0.5.0, 13.2.0.0.0, 13.3.0.0.0
- Enterprise Manager for Fusion Middleware, versions 13.2, 13.3
- Enterprise Manager for Virtualization, versions 13.1, 13.2, 13.3
- Enterprise Manager Ops Center, versions 12.3.3, 12.4.0
- Instantis EnterpriseTrack, versions 17.1, 17.2, 17.3
- JD Edwards EnterpriseOne Tools, version 9.2
- JD Edwards World Security, versions A9.3, A9.3.1, A9.4
- MICROS Retail XBRi Loss Prevention, versions 10.8.0 - 10.8.3
- MICROS Retail-J, versions 12.1.0, 12.1.1, 12.1.2, 13.1
- MySQL Enterprise Monitor, versions 4.0.9 and prior, 8.0.14 and prior
- MySQL Server, versions 5.6.44 and prior, 5.7.26 and prior, 8.0.16 and prior
- MySQL Workbench, versions 8.0.16 and prior
- Oracle Agile Engineering Data Management, versions 6.2.0, 6.2.1
- Oracle Agile PLM, versions 9.3.3, 9.3.4, 9.3.5, 9.3.6
- Oracle Application Testing Suite, versions 13.1, 13.2, 13.3
- Oracle Banking Platform, versions 2.4.0 - 2.7.1
- Oracle Berkeley DB, versions 12.1.6.1.23, 12.1.6.1.26, 12.1.6.1.29, 12.1.6.1.36, 12.1.6.2.23, 12.1.6.2.32
- Oracle BI Publisher, version 11.1.1.9.0
- Oracle Business Intelligence Enterprise Edition, versions 11.1.1.9.0, 12.2.1.4.0
- Oracle Clusterware, version 12.1.0.2.0
- Oracle Communications Application Session Controller, versions 3.7.1, 3.8.0
- Oracle Communications Billing and Revenue Management, versions 7.5, 12.0

- Oracle Communications Converged Application Server, versions 5.1, 7.0, 7.1
- Oracle Communications Converged Application Server - Service Controller, versions 6.0, 6.1
- Oracle Communications Convergence, version 3.0.2
- Oracle Communications Diameter Signaling Router (DSR), versions 8.0, 8.1, 8.2, 8.3
- Oracle Communications EAGLE (Software), versions 46.5, 46.6, 46.7
- Oracle Communications Instant Messaging Server, version 10.0.1.2.0
- Oracle Communications Interactive Session Recorder, versions 6.0, 6.1, 6.2
- Oracle Communications Messaging Server, versions 8.0.2, 8.1.0
- Oracle Communications Online Mediation Controller, version 6.1
- Oracle Communications Unified, version 8.0.0.2.0
- Oracle Data Integrator, version 12.2.1.3.0
- Oracle Database Server, versions 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c, 19c
- Oracle Demantra Demand Management, version 7.3.1.5.2
- Oracle E-Business Suite, versions 12.1.1 - 12.1.3, 12.2.3 - 12.2.8
- Oracle Endeca Information Discovery Integrator, version 3.2.0
- Oracle Endeca Server, version 7.7.0
- Oracle Enterprise Manager Base Platform, versions 12.1.0.5.0, 13.2.0.0.0, 13.3.0.0.0
- Oracle Enterprise Repository, version 12.1.3.0.0
- Oracle Financial Services - Regulatory Reporting for Reserve Bank of India - Lombard Risk Integration Pack, version 8.0.7
- Oracle Financial Services - Regulatory Reporting for US Federal Reserve - Lombard Risk Integration Pack, versions 8.0.4 - 8.0.7
- Oracle Financial Services Analytical Applications Infrastructure, versions 7.3.3 - 7.3.5, 8.0.2 - 8.0.8
- Oracle Financial Services Analytical Applications Reconciliation Framework, versions 8.0.4 - 8.0.7
- Oracle Financial Services Asset Liability Management, versions 8.0.4 - 8.0.7
- Oracle Financial Services Basel Regulatory Capital Basic, versions 8.0.4 - 8.0.7
- Oracle Financial Services Basel Regulatory Capital Internal Ratings Based Approach, versions 8.0.4 - 8.0.7
- Oracle Financial Services Data Foundation, versions 8.0.4 - 8.0.8
- 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 Institutional Performance Analytics, versions 8.0.4 - 8.0.7
- Oracle Financial Services Liquidity Risk Management, versions 8.0.1, 8.0.2, 8.0.4, 8.0.5, 8.0.6
- Oracle Financial Services Liquidity Risk Measurement and Management, versions 8.0.7, 8.0.8
- 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, 8.0.8
- Oracle Financial Services Price Creation and Discovery, versions 8.0.4 - 8.0.7
- Oracle Financial Services Profitability Management, versions 8.0.4 - 8.0.7
- Oracle Financial Services Regulatory Reporting for European Banking Authority, versions 8.0.6, 8.0.7
- Oracle Financial Services Regulatory Reporting for European Banking Authority - Integration Pack for Lombard Risk, versions 8.0.6, 8.0.7
- Oracle Financial Services Regulatory Reporting for US Federal Reserve, versions 8.0.4 - 8.0.7
- Oracle Financial Services Retail Customer Analytics, versions 8.0.4 - 8.0.6
- Oracle Financial Services Revenue Management and Billing, versions 2.4.0.0, 2.4.0.1
- Oracle FLEXCUBE Core Banking, versions 5.2.0, 11.6.0, 11.7.0, 11.8.0
- Oracle FLEXCUBE Enterprise Limits and Collateral Management, versions 12.0, 12.1
- Oracle FLEXCUBE Investor Servicing, versions 12.0.1, 12.0.3, 12.0.4, 12.1.0, 12.3.0, 12.4.0, 14.0.0, 14.1.0
- Oracle FLEXCUBE Private Banking, versions 12.0.1, 12.0.3, 12.1.0
- Oracle FLEXCUBE Universal Banking, versions 12.0.1 - 12.0.3, 12.1.0 - 12.4.0, 14.0.0 - 14.2.0
- Oracle Global Lifecycle Management OPatchAuto, versions prior to 12.2.0.1.14
- Oracle GraalVM Enterprise Edition, version 19.0.0
- Oracle Hospitality Gift and Loyalty, versions 9.0.0, 9.1.0
- Oracle Hospitality Guest Access, versions 4.2, 4.2.1
- Oracle Hospitality Simphony, version 18.2.1
- Oracle Hospitality Suite8, versions 8.9.6, 8.10.2, 8.11 - 8.14
- Oracle HTTP Server, versions 12.1.3.0.0, 12.2.1.3.0
- Oracle Hyperion Planning, version 11.1.2.4
- Oracle Hyperion Workspace, version 11.1.2.4
- Oracle Identity Manager, versions 11.1.2.3.0, 12.2.1.3.0
- Oracle Insurance Allocation Manager for Enterprise Profitability, version 8.0.8
- Oracle Insurance Calculation Engine, versions 9.7, 10.0, 10.1, 10.2
- Oracle Insurance Data Foundation, versions 8.0.4 - 8.0.7
- Oracle Insurance IFRS 17 Analyzer, versions 8.0.6, 8.0.7
- Oracle Insurance Performance Insight, version 8.0.7
- Oracle Insurance Policy Administration J2EE, versions 10.0, 10.1, 10.2, 11.0
- Oracle Insurance Rules Palette, versions 10.0, 10.1, 10.2, 11.0
- Oracle Java SE, versions 7u221, 8u212, 11.0.3, 12.0.1
- Oracle Java SE Embedded, version 8u211
- Oracle Outside In Technology, version 8.5.4
- Oracle Retail Advanced Inventory Planning, version 15.0
- Oracle Retail Customer Management and Segmentation Foundation, versions 16.0, 17.0, 18.0
- Oracle Retail Financial Integration, versions 14.0, 14.1, 15.0, 16.0
- Oracle Retail Integration Bus, versions 15.0, 16.0

- Oracle Retail Order Broker, versions 5.2, 15.0
- Oracle Retail Order Management System, version 5.0
- Oracle Retail Predictive Application Server, versions 14.0.3.26, 14.1.3.37, 15.0.3.100, 16.0
- Oracle Retail Service Backbone, version 16.0.1
- Oracle Retail Xstore Office, versions 7.0, 7.1
- Oracle Retail Xstore Point of Service, versions 7.0, 7.1, 15.0, 16.0, 17.0, 18.0
- Oracle Security Service, versions 11.1.1.9.0, 12.1.3.0.0, 12.2.1.3.0
- Oracle SOA Suite, version 12.2.1.3.0
- Oracle Solaris, versions 10, 11.3, 11.4
- Oracle Transportation Management, version 6.3.7
- Oracle Utilities Advanced Spatial and Operational Analytics, version 2.7.0.1
- Oracle Utilities Framework, versions 4.3.0.2.0 - 4.3.0.6.0, 4.4.0.0.0
- Oracle VM VirtualBox, versions prior to 5.2.32, prior to 6.0.10
- 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
- PeopleSoft Enterprise FIN Project Costing, 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 Analytics, version 18.8
- Primavera Gateway, versions 15.2, 16.2, 17.12, 18.8
- Primavera Unifier, versions 16.1, 16.2, 17.7 - 17.12, 18.8
- Services Tools Bundle, version 19.2
- Siebel Applications, versions 19.0 and prior
- StorageTek Tape Analytics SW Tool, version 2.3.0
- Sun ZFS Storage Appliance Kit (AK), version 8.8.3
- System Utilities, version 19.1
- Tape Virtual Storage Manager GUI, version 6.2

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**

Solution:

Rw-CSIRT is strongly recommending **users** and **IT administrators** to:

- 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.

Affected users should: contact RW-CSIRT: Call **4045** or write to **security@risa.rw** to help for analyzing the source of the incident and recommendation.

The reference of a full list of all vulnerabilities can be found on the links below:

https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html
https://www.jpcert.or.jp/english/at/2019/at190030.html

National Computer Security and Incident Response Team (Rw-CSIRT) Mission

Rw-CSIRT mission is to build cyber-security capabilities to increase the capacity of "early **Detection**, **Prevention**, **Response** to incidents and **Reduce** Vulnerability" and raise cyber security awareness in public.