PTA CERT for Telecom Sector

Security Advisory-No: 35

29, Jan 2019

Classification: Critical Security Patches

Name: Multiple Vulnerabilities

Distribution: The vulnerabilities can be exploited to the following Products of Oracle

- Enterprise Manager Base Platform, versions 12.1.0.5, 13.2, 13.3
- Enterprise Manager for Virtualization, versions 13.2.2, 13.2.3, 13.3.1
- Enterprise Manager Ops Center, versions 12.2.2, 12.3.3
- Hyperion BI+, version 11.1.2.4
- Java Advanced Management Console, version 2.12
- JD Edwards Enterprise One Tools, version 9.2
- JD Edwards World Security, versions A9.3, A9.3.1, A9.4
- MySQL Connectors, versions 2.1.8 and prior, 8.0.13 and prior
- MySQL Enterprise Monitor, versions 4.0.7 and prior, 8.0.13 and prior
- MySQL Server, versions 5.6.42 and prior, 5.7.24 and prior, 8.0.13 and prior
- MySQL Workbench, versions 8.0.13 and prior
- 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 Product Lifecycle Management for Process, versions 6.2.0.0, 6.2.1.0, 6.2.2.0, 6.2.3.0, 6.2.3.1
- Oracle API Gateway, version 11.1.2.4.0
- Oracle Application Testing Suite, versions 12.5.0.3, 13.1.0.1, 13.2.0.1, 13.3.0.1
- Oracle Argus Safety, versions 8.1, 8.2
- Oracle Banking Platform, versions 2.5.0, 2.6.0, 2.6.1, 2.6.2
- Oracle Business Process Management Suite, versions 11.1.1.9.0, 12.1.3.0.0, 12.2.1.3.0
- Oracle Communications Billing and Revenue Management, versions 7.5, 12.0
- Oracle Communications Converged Application Server, versions prior to 7.0.0.1
- Oracle Communications Converged Application Server - Service Controller, version 6.1
- Oracle Communications Diameter Signaling Router (DSR), versions prior to 8.3
- Oracle Communications Online Mediation Controller, version 6.1
- Oracle Communications Performance Intelligence Center (PIC) Software, versions prior to 10.2.1
- Oracle Communications Policy Management, versions prior to 12.5
- Oracle Communications Service Broker, version 6.0
- Oracle Communications Services Gatekeeper, versions prior to 6.1.0.4.0
- Oracle Communications Session Border Controller, versions SCz7.4.0, SCz7.4.1, SCz8.0.0, SCz8.1.0
- Oracle Communications Unified Inventory Management, versions prior to 7.4.0
- Oracle Communications Unified Session Manager, version SCz7.3.5
- Oracle Communications WebRTC Session Controller, versions prior to 7.2
- Oracle Database Server, versions 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c
- 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, 12.2.8
- Oracle Endeca Server, version 7.7.0
- Oracle Enterprise Communications Broker, versions PCz2.1, PCz2.2, PCz3.0
- Oracle Enterprise Repository, version 12.1.3.0.0
- Oracle Enterprise Session Border Controller, versions ECz7.4.0, ECz7.5.0, ECz8.0.0, ECz8.1.0
- Oracle Financial Services Analytical Applications Infrastructure, versions 7.3.3, 7.3.5, 8.0.1, 8.0.2, 8.0.3, 8.0.4, 8.0.5, 8.0.6, 8.0.7
- Oracle FLEXCUBE Direct Banking, version 12.0.2
- Oracle FLEXCUBE Investor Servicing, versions 12.0.4, 12.1.0, 12.3.0, 12.4.0, 14.0.0

- Oracle Fusion Middleware Map Viewer, version 12.2.1.3.0
- Oracle Golden Gate Application Adapters, version 12.3.2.1.1
- Oracle Health Sciences Information Manager, version 3.0
- Oracle Healthcare Foundation, versions 7.1, 7.2
- Oracle Healthcare Master Person Index, versions 3.0, 4.0
- Oracle Hospitality Cruise Fleet Management, version 9.0.10
- Oracle Hospitality Cruise Shipboard Property Management System, version 8.0.8
- Oracle Hospitality Reporting and Analytics, version 9.1.0
- Oracle Hospitality Simphony, version 2.10
- Oracle HTTP Server, version 12.2.1.3
- Oracle Insurance Calculation Engine, version 10.2
- Oracle Insurance Insbridge Rating and Underwriting, versions 5.2, 5.4, 5.5
- Oracle Insurance Policy Administration J2EE, versions 10.0, 10.2
- Oracle Insurance Rules Palette, versions 10.0, 10.2
- Oracle Java SE, versions 7u201, 8u192, 11.0.1
- Oracle Java SE Embedded, version 8u191
- Oracle Managed File Transfer, versions 12.2.1.3.0, 19.1.0.0.0
- Oracle Outside In Technology, versions 8.5.3, 8.5.4
- Oracle Reports Developer, version 12.2.1.3
- Oracle Retail Back Office, versions 13.3, 13.4, 14.0, 14.1
- Oracle Retail Central Office, versions 13.3, 13.4, 14.0, 14.1
- Oracle Retail Convenience and Fuel POS Software, version 2.8.1
- Oracle Retail Customer Insights, versions 15.0, 16.0
- Oracle Retail Integration Bus, version 17.0
- Oracle Retail Merchandising System, version 14.1
- Oracle Retail Returns Management, versions 13.3, 13.4, 14.0, 14.1
- Oracle Retail Sales Audit, version 15.0
- Oracle Retail Service Backbone, versions 13.1, 13.2, 14.0, 14.1, 15.0, 16.0
- Oracle Retail Workforce Management Software, versions 1.60.9, 1.64.0
- Oracle Retail Xstore Payment, version 3.3
- Oracle Secure Global Desktop (SGD), version 5.4
- Oracle Service Architecture Leveraging Tuxedo, versions 12.1.3.0.0, 12.2.2.0.0
- Oracle SOA Suite, versions 12.1.3.0.0, 12.2.1.3.0
- Oracle Solaris, versions 10, 11
- Oracle Transportation Management, versions 6.3.7, 6.4.1, 6.4.2, 6.4.3
- Oracle Utilities Framework, version 4.3.0.1-4.3.0.4
- Oracle Utilities Network Management System, versions 1.12.0.3, 2.3.0.0, 2.3.0.1, 2.3.0.2
- Oracle VM VirtualBox, versions prior to 5.2.24, prior to 6.0.2
- Oracle Web Cache, version 11.1.1.9.0
- Oracle WebCenter Portal, versions 11.1.1.9.0, 12.2.1.3.0
- Oracle WebCenter Sites, version 11.1.1.8.0
- Oracle WebLogic Server, versions 10.3.6.0, 12.1.3.0, 12.2.1.3
- OSS Support Tools, versions prior to 19.1
- PeopleSoft Enterprise CC Common Application Objects, version 9.2
- PeopleSoft Enterprise CS Campus Community, versions 9.0, 9.2
- PeopleSoft Enterprise HCM eProfile Manager Desktop, version 9.2
- PeopleSoft Enterprise PeopleTools, versions 8.55, 8.56, 8.57
- PeopleSoft Enterprise SCM eProcurement, version 9.2
- 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, 17.1-17.12, 18.8
- Siebel Applications, versions 18.10, 18.11
- Sun ZFS Storage Appliance Kit (AK), versions prior to 8.8.2
- Tape Library ACSLS, version 8.4

Exploited Vulnerabilities: A collection of Critical Patches has updated by Oracle to overcome multiple security vulnerabilities in above-listed products; Oracle strongly recommends that users above listed products should update critical Patches as soon as possible.

Recommendations:

1) Administrator may use following official patches to fix the aforementioned vulnerabilities:
    - https://www.oracle.com/technetwork/security-advisory/cpujan2019-5072801.html
2) Whenever possible, run software with minimal access rights and privileges.
3) Only use licensed software and avoids download/use of crack and pirated software.
4) In case of any incident, please report to this office.