The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

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:
01/19/2021

SUBJECT:
Oracle Quarterly Critical Patches Issued January 19, 2021

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

SYSTEMS AFFECTED:

- 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
- Enterprise Manager Base Platform, versions 13.2.1.0, 13.3.0.0, 13.4.0.0
- Enterprise Manager for Fusion Applications, version 13.3.0.0
- Enterprise Manager Ops Center, version 12.4.0.0
- Hyperion Financial Reporting, version 11.1.2.4
- Hyperion Infrastructure Technology, version 11.1.2.4
- Instantis EnterpriseTrack, versions 17.1-17.3
- JD Edwards EnterpriseOne Orchestrator, versions prior to 9.2.5.1
- JD Edwards EnterpriseOne Tools, versions prior to 9.2.5.0
- MySQL Client, versions 5.6.50 and prior, 5.7.32 and prior, 8.0.22 and prior
- MySQL Enterprise Monitor, versions 8.0.22 and prior
- MySQL Server, versions 5.6.50 and prior, 5.7.32 and prior, 8.0.22 and prior
- MySQL Workbench, versions 8.0.22 and prior
- Oracle Adaptive Access Manager, version 11.1.2.3.0
- Oracle Agile Engineering Data Management, version 6.2.1.0
- Oracle Agile PLM, versions 9.3.5, 9.3.6
- Oracle Agile Product Lifecycle Management for Process, version 6.1
- Oracle Application Express Opportunity Tracker, versions prior to 20.2
- Oracle Application Express Survey Builder, versions prior to 20.2
- Oracle Application Testing Suite, version 13.3.0.1
- Oracle Argus Safety, version 8.2.2
- Oracle BAM (Business Activity Monitoring), versions 11.1.1.9.0, 12.2.1.3.0
- Oracle Banking Corporate Lending Process Management, versions 14.1.0, 14.3.0, 14.4.0

- Oracle Banking Credit Facilities Process Management, versions 14.1.0, 14.3.0, 14.4.0
- Oracle Banking Extensibility Workbench, versions 14.3.0, 14.4.0
- Oracle Banking Liquidity Management, versions 14.0.0-14.4.0
- Oracle Banking Payments, version 14.4.0
- Oracle Banking Platform, versions 2.4.0, 2.4.1, 2.6.2, 2.7.0, 2.7.1, 2.8.0, 2.9.0
- Oracle Banking Supply Chain Finance, versions 14.2.0-14.4.0
- Oracle Banking Trade Finance Process Management, versions 14.1.0, 14.3.0, 14.4.0
- Oracle Banking Virtual Account Management, versions 14.1.0, 14.3.0, 14.4.0
- Oracle BI Publisher, versions 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0
- 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
- Oracle Business Process Management Suite, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle Coherence, versions 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0
- Oracle Communications Application Session Controller, version 3.9m0p2
- Oracle Communications ASAP, version 7.3
- Oracle Communications BRM - Elastic Charging Engine, versions 11.3.0.9, 12.0.0.3
- Oracle Communications Calendar Server, version 8.0.0.4.0
- Oracle Communications Contacts Server, version 8.0.0.5.0
- Oracle Communications Diameter Signaling Router (DSR), versions 8.0.0-8.2.2
- Oracle Communications Element Manager, versions 8.2.1.0-8.2.2.1
- Oracle Communications MetaSolv Solution, versions 6.3.0-6.3.1
- Oracle Communications Network Charging and Control, versions 6.0.1, 12.0.2
- Oracle Communications Operations Monitor, versions 3.4, 4.1, 4.2, 4.3
- Oracle Communications Performance Intelligence Center (PIC) Software, version 10.4.0.2
- Oracle Communications Session Report Manager, versions 8.2.1.0-8.2.2.1
- Oracle Complex Maintenance, Repair, and Overhaul, versions 11.5.10, 12.1, 12.2
- Oracle Configurator, versions 12.1, 12.2
- Oracle Data Integrator, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0
- Oracle Database Server, versions 12.1.0.2, 12.2.0.1, 18c, 19c
- Oracle E-Business Suite, versions 12.1.1-12.1.3, 12.2.3-12.2.10
- Oracle Endeca Information Discovery Integrator, version 3.2.0.0
- Oracle Enterprise Communications Broker, versions 3.1, 3.2
- Oracle Enterprise Data Quality, versions 11.1.1.9.0, 12.2.1.3.0
- Oracle Enterprise Repository, version 11.1.1.7.0
- Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.6-8.1.0
- Oracle Financial Services Asset Liability Management, versions 8.0.7, 8.1.0
- Oracle Financial Services Data Integration Hub, versions 8.0.3, 8.0.6
- Oracle Financial Services Funds Transfer Pricing, versions 8.0.6, 8.0.7, 8.1.0
- Oracle Financial Services Market Risk Measurement and Management, version 8.0.6
- Oracle Financial Services Profitability Management, versions 8.0.6, 8.0.7, 8.1.0
- Oracle Financial Services Revenue Management and Billing, versions 2.9.0.0, 2.9.0.1
- Oracle FLEXCUBE Core Banking, versions 11.5.0-11.9.0
- Oracle FLEXCUBE Universal Banking, version 14.4.0
- Oracle Fusion Middleware MapViewer, version 12.2.1.3.0
- Oracle Global Lifecycle Management OPatch
- Oracle Global Lifecycle Manager
- Oracle GoldenGate Application Adapters, version 19.1.0.0.0

- Oracle GraalVM Enterprise Edition, versions 19.3.4, 20.3.0
- Oracle Health Sciences Information Manager, version 3.0.1
- Oracle Healthcare Master Person Index, version 4.0.2.5
- Oracle Hospitality Reporting and Analytics, version 9.1.0
- Oracle Hospitality Simphony, versions 18.2.7.2, 19.1.3
- Oracle Insurance Allocation Manager for Enterprise Profitability, version 8.1.0
- Oracle Insurance Insbridge Rating and Underwriting, versions 5.0.0.20, 5.1.1.3
- Oracle Insurance Policy Administration, versions 10.2.0, 10.2.4, 11.0.2, 11.1.0-11.3.0
- Oracle Insurance Rules Palette, versions 10.2.0, 10.2.4, 11.0.2, 11.1.0-11.3.0
- Oracle Java SE, versions 7u281, 8u271
- Oracle Java SE Embedded, version 8u271
- Oracle Managed File Transfer, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle Outside In Technology, versions 8.5.4, 8.5.5
- Oracle Real-Time Decision Server, version 3.2.1.0
- Oracle Retail Assortment Planning, version 16.0.3
- Oracle Retail Bulk Data Integration, versions 15.0.3, 16.0.3
- Oracle Retail Customer Management and Segmentation Foundation, versions 16.0, 17.0, 18.0, 19.0
- Oracle Retail Extract Transform and Load, versions 13.2.5, 13.2.8
- Oracle Retail Financial Integration, versions 14.1.3, 15.0.3, 16.0.3
- Oracle Retail Integration Bus, versions 14.1.3, 15.0.3, 16.0.3
- Oracle Retail Invoice Matching, versions 13.2, 14.0, 14.1
- Oracle Retail Merchandising System, version 15.0
- Oracle Retail Order Broker, versions 15.0, 16.0
- Oracle Retail Order Broker Cloud Service, version 15.0
- Oracle Retail Sales Audit, version 14.1
- Oracle Retail Service Backbone, versions 14.1.3, 15.0.3, 16.0.3
- Oracle Retail Store Inventory Management, versions 14.0.4.0, 14.1.3.0, 14.1.3.9, 15.0.3.0, 16.0.3.0
- Oracle SD-WAN Edge, version 9.0
- Oracle Secure Backup
- Oracle Transportation Management, version 1.4.3
- Oracle Utilities Framework, versions 4.2.0.2.0, 4.2.0.3.0, 4.3.0.1.0-4.3.0.6.0, 4.4.0.0.0, 4.4.0.2.0
- Oracle VM VirtualBox, versions prior to 6.1.18
- Oracle WebCenter Portal, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0
- Oracle WebCenter Sites, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle WebLogic Server, versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0
- Oracle ZFS Storage Appliance Kit, version 8.8
- PeopleSoft Enterprise FIN Payables, version 9.2
- PeopleSoft Enterprise HCM Human Resources, version 9.2
- PeopleSoft Enterprise PeopleTools, versions 8.56, 8.57, 8.58
- Primavera Gateway, versions 16.2.0-16.2.11, 17.12.0-17.12.9, 18.8.0-18.8.10, 19.12.0-19.12.10
- Primavera P6 Enterprise Project Portfolio Management, versions 16.1.0-16.2.20, 17.1.0-17.12.19, 18.1.0-18.8.21, 19.12.0-19.12.10
- Primavera Unifier, versions 16.1, 16.2, 17.7-17.12, 18.8, 19.12, 20.12

- Siebel Applications, versions 20.12 and prior
- StorageTek Tape Analytics SW Tool, version 2.3.1

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/security-alerts/cpujan2021.html