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

https://www.cisa.gov/tlp

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:

10/19/2021

SUBJECT:

Oracle Quarterly Critical Patches Issued October 19, 2021

OVERVIEW:

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

SYSTEMS AFFECTED:

- Affected Products and Versions
- Enterprise Manager Base Platform, versions 13.4.0.0, 13.5.0.0
- Enterprise Manager for Oracle Database, version 13.4.0.0
- Enterprise Manager Ops Center, version 12.4.0.0
- Essbase Administration Services, versions prior to 11.1.2.4.46
- Hyperion Financial Management, versions 11.1.2.4, 11.2.6.0
- Hyperion Financial Reporting, versions 11.1.2.4, 11.2.6.0
- Hyperion Infrastructure Technology, version 11.2.6.0
- Hyperion Planning, versions 11.1.2.4, 11.2.6.0
- Instantis EnterpriseTrack, versions 17.1, 17.2, 17.3
- JD Edwards EnterpriseOne Orchestrator, versions prior to 9.2.6.0
- JD Edwards EnterpriseOne Tools, versions prior to 9.2.6.0
- JD Edwards World Security, version A9.4
- MySQL Client, versions 8.0.26 and prior
- MySQL Cluster, versions 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior, 8.0.26 and prior
- MySQL Connectors, versions 8.0.26 and prior
- MySQL Enterprise Monitor, versions 8.0.25 and prior
- MySQL Server, versions 5.7.35 and prior, 8.0.26 and prior
- MySQL Workbench, versions 8.0.26 and prior
- Oracle Agile PLM, versions 9.3.3, 9.3.6
- Oracle Application Express, versions prior to 21.1.0
- Oracle Application Testing Suite, version 13.3.0.1
- Oracle Autovue for Agile Product Lifecycle Management, version 21.0.2
- Oracle Banking Cash Management, versions 14.2, 14.3, 14.5
- Oracle Banking Corporate Lending Process Management, versions 14.2, 14.3, 14.5
- Oracle Banking Credit Facilities Process Management, versions 14.2, 14.3, 14.5

- Oracle Banking Enterprise Default Management, versions 2.10.0, 2.12.0
- Oracle Banking Extensibility Workbench, versions 14.2, 14.3, 14.5
- Oracle Banking Platform, versions 2.6.2, 2.7.1, 2.9.0, 2.12.0
- Oracle Banking Supply Chain Finance, versions 14.2, 14.3, 14.5
- Oracle Banking Trade Finance Process Management, versions 14.2, 14.3, 14.5
- Oracle Banking Virtual Account Management, versions 14.2, 14.3, 14.5
- Oracle Business Activity Monitoring, versions 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, 12.2.1.3.0, 12.2.1.4.0
- Oracle Commerce Guided Search, version 11.3.2
- Oracle Commerce Merchandising, version 11.3.2
- Oracle Communications Application Session Controller, version 3.9
- Oracle Communications Billing and Revenue Management, versions 7.5.0.0.0, 12.0.0.3.0
- Oracle Communications BRM - Elastic Charging Engine, version 12.0.0.3
- Oracle Communications Calendar Server, version 8.0.0.6.0
- Oracle Communications Cloud Native Core Network Repository Function, version 1.14.0
- Oracle Communications Cloud Native Core Policy, version 1.11.0
- Oracle Communications Control Plane Monitor, versions 3.4, 4.2, 4.3, 4.4
- Oracle Communications Converged Application Server - Service Controller, version 6.2
- Oracle Communications Design Studio, version 7.4.2
- Oracle Communications Diameter Signaling Router, versions 8.0.0.0-8.5.0.0
- Oracle Communications EAGLE
- Oracle Communications EAGLE FTP Table Base Retrieval, version 4.5
- Oracle Communications EAGLE LNP Application Processor, versions 46.7, 46.8, 46.9
- Oracle Communications Element Manager, versions 8.2.0.0-8.2.4.0
- Oracle Communications Fraud Monitor, versions 3.4-4.4
- Oracle Communications Interactive Session Recorder, version 6.4
- Oracle Communications LSMS, versions 13.1-13.4
- Oracle Communications Messaging Server, version 8.1
- Oracle Communications MetaSolv Solution, version 6.3.1
- Oracle Communications Offline Mediation Controller, version 12.0.0.3.0
- Oracle Communications Operations Monitor, versions 3.4, 4.2, 4.3, 4.4
- Oracle Communications Policy Management, version 12.5.0
- Oracle Communications Pricing Design Center, version 12.0.0.3.0
- Oracle Communications Services Gatekeeper, version 7.0
- Oracle Communications Session Border Controller, versions 8.4, 9.0
- Oracle Communications Session Report Manager, versions 8.0.0.0-8.2.5.0
- Oracle Communications Session Route Manager, versions 8.0.0.0-8.2.5.0
- Oracle Data Integrator, version 12.2.1.4.0
- Oracle Database Server, versions 12.1.0.2, 12.2.0.1, 19c, 21c
- Oracle Documaker, versions 12.6.0-12.6.4
- Oracle E-Business Suite, versions 12.1.1-12.1.3, 12.2.3-12.2.10
- Oracle Enterprise Communications Broker, versions 3.2, 3.3
- Oracle Enterprise Repository, version 11.1.1.7.0
- Oracle Enterprise Telephony Fraud Monitor, versions 3.4, 4.2, 4.3, 4.4
- Oracle Ethernet Switch ES2-64, Oracle Ethernet Switch ES2-72, version 2.0.0.14
- Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.6-8.1.1
- Oracle Financial Services Enterprise Case Management, versions 8.0.7.2.0, 8.0.8.1.0

- Oracle Financial Services Model Management and Governance, versions 8.0.8.0.0-8.1.0.0.0
- Oracle FLEXCUBE Core Banking, versions 11.7, 11.8, 11.9, 11.10
- Oracle Global Lifecycle Management OPatch
- Oracle GoldenGate, versions prior to 19.1.0.0.0.210420
- Oracle GoldenGate Application Adapters, version 19.1.0.0.0
- Oracle GraalVM Enterprise Edition, versions 20.3.3, 21.2.0
- Oracle Graph Server and Client, versions prior to 21.3.0
- Oracle Health Sciences Central Coding, versions 6.2.0, 6.3.0
- Oracle Health Sciences InForm, version 6.3.0
- Oracle Healthcare Data Repository, versions 7.0.2, 8.1.0
- Oracle Healthcare Foundation, versions 7.3, 8.0, 8.1
- Oracle Hospitality Cruise Shipboard Property Management System, version 20.1.0
- Oracle HTTP Server, versions 11.1.1.9.0, 12.2.1.4.0
- Oracle Insurance Calculation Engine, versions 11.0.0-11.3.1
- Oracle Insurance Policy Administration, versions 11.0.0-11.3.1
- Oracle Java SE, versions 7u311, 8u301, 11.0.12, 17
- Oracle NoSQL Database
- Oracle Outside In Technology, version 8.5.5
- Oracle Real User Experience Insight, versions 13.4.1.0, 13.5.1.0
- Oracle Real-Time Decision Server, versions 3.2.0.0, 11.1.1.9.0
- Oracle REST Data Services, versions prior to 21.3
- Oracle Retail Advanced Inventory Planning, versions 14.1, 15.0, 16.0
- Oracle Retail Assortment Planning, version 16.0
- Oracle Retail Back Office, versions 14.0, 14.1
- Oracle Retail Bulk Data Integration, versions 16.0.3, 19.0.1
- Oracle Retail Central Office, versions 14.0, 14.1
- Oracle Retail Customer Management and Segmentation Foundation, versions 16.0-19.0
- Oracle Retail Extract Transform and Load, version 13.2.8
- Oracle Retail Financial Integration, versions 14.1.3.2, 15.0.4.0, 16.0.3.0
- Oracle Retail Integration Bus, versions 14.1.3.2, 15.0.4.0, 16.0.3.0, 19.0.1.0
- Oracle Retail Merchandising System, versions 15.0.3, 19.0.1
- Oracle Retail Point-of-Service, versions 14.0, 14.1
- Oracle Retail Predictive Application Server, versions 14.1.3, 15.0.3, 16.0.3
- Oracle Retail Returns Management, versions 14.0, 14.1
- Oracle Retail Service Backbone, versions 14.1.3.2, 15.0.4.0, 16.0.3.0, 19.0.1.0
- Oracle Retail Store Inventory Management, versions 14.1, 15.0, 16.0
- Oracle Secure Backup, versions prior to 18.1.0.1.0
- Oracle Secure Global Desktop, version 5.6
- Oracle Solaris, version 11
- Oracle Spatial Studio
- Oracle SQL Developer
- Oracle Transportation Management, version 6.4.3
- 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, 4.4.0.3.0
- Oracle VM VirtualBox, versions prior to 6.1.28
- Oracle WebCenter Portal, versions 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 WebLogic Server Proxy Plug-In, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle ZFS Storage Appliance Kit, version 8.8
- PeopleSoft Enterprise CC Common Application Objects, version 9.2
- PeopleSoft Enterprise CS Academic Advisement, version 9.2
- PeopleSoft Enterprise CS Campus Community, versions 9.0, 9.2
- PeopleSoft Enterprise CS SA Integration Pack, versions 9.0, 9.2
- PeopleSoft Enterprise CS Student Records, version 9.2
- PeopleSoft Enterprise PeopleTools, versions 8.57, 8.58, 8.59
- PeopleSoft Enterprise SCM, version 9.2
- Primavera Gateway, versions 17.12.0-17.12.11, 18.8.0-18.8.12, 19.12.0-19.12.11, 20.12.0-20.12.7
- Primavera Unifier, versions 17.7-17.12, 18.8, 19.12, 20.12
- Siebel Applications, versions 21.9 and prior
- Tekelec Platform Distribution, versions 7.4.0-7.7.1
- Tekelec Virtual Operating Environment, versions 3.4.0-3.7.1

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

REFERENCES:
https://www.oracle.com/security-alerts/cpuoct2021.html