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
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
10/19/2022

SUBJECT:
Oracle Quarterly Critical Patches Issued October 19, 2022

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, version 13.4.1.0.0
- Big Data Spatial and Graph
- Enterprise Manager Base Platform, versions 13.4.0.0, 13.5.0.0
- Enterprise Manager for Virtualization, versions 13.4.0.0, 13.5.0.0
- Enterprise Manager Ops Center, version 12.4.0.0
- JD Edwards EnterpriseOne Orchestrator, versions 9.2.6.4 and prior
- JD Edwards EnterpriseOne Tools, versions 9.2.6.4 and prior
- MySQL Connectors, versions 8.0.30 and prior
- MySQL Enterprise Backup, versions 4.1.4 and prior
- MySQL Enterprise Monitor, versions 8.0.31 and prior
- MySQL Installer, versions 1.6.3 and prior
- MySQL Server, versions 5.7.39 and prior, 8.0.30 and prior
- MySQL Shell, versions 8.0.30 and prior
- MySQL Workbench, versions 8.0.30 and prior
- Oracle Access Manager, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle Agile Engineering Data Management, version 6.2.1.0
- Oracle Agile PLM, version 9.3.6
- Oracle Airlines Data Model
- Oracle Application Express
- Oracle AutoVue, version 21.0.2
- Oracle Autovue for Agile Product Lifecycle Management, version 21.0.2
- Oracle Banking Enterprise Default Management, version 2.12.0

- Oracle Banking Loans Servicing, versions 2.8.0, 2.12.0
- Oracle Banking Party Management, version 2.7.0
- Oracle Banking Platform, versions 2.7.1, 2.9.0, 2.12.0
- Oracle BI Publisher, versions 5.9.0.0, 6.4.0.0.0, 12.2.1.3.0, 12.2.1.4.0
- Oracle Business Activity Monitoring(Oracle BAM), versions 12.2.1.3.0, 12.2.1.4.0
- Oracle Business Intelligence Enterprise Edition, versions 5.9.0.0, 6.4.0.0
- Oracle Business Process Management Suite, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle Coherence, versions 12.2.1.4.0, 14.1.1.0.0
- Oracle Commerce Platform, versions 11.3.0-11.3.2
- Oracle Communications Billing and Revenue Management, versions 12.0.0.4.0-12.0.0.7.0
- Oracle Communications Cloud Native Core Binding Support Function, version 22.3.0
- Oracle Communications Cloud Native Core Console, version 22.2.0
- Oracle Communications Cloud Native Core Network Exposure Function, versions 22.2.1, 22.3.0
- Oracle Communications Cloud Native Core Network Function Cloud Native Environment, versions 1.9.0, 22.1, 22.1.0, 22.2, 22.2.0, 22.2.1
- Oracle Communications Cloud Native Core Network Repository Function, version 22.2.2
- Oracle Communications Cloud Native Core Policy, version 22.3.0
- Oracle Communications Cloud Native Core Security Edge Protection Proxy, versions 22.1.1, 22.2.0, 22.2.1, 22.3.0
- Oracle Communications Cloud Native Core Service Communication Proxy, versions 22.2.3, 22.3.1, 22.4.0
- Oracle Communications Cloud Native Core Unified Data Repository, versions 22.1.1, 22.2.1, 22.3.0
- Oracle Communications Converged Application Server - Service Controller, version 6.2
- Oracle Communications Convergence, version 3.0.3.0
- Oracle Communications Convergent Charging Controller, versions 6.0.1.0.0, 12.0.1.0.0-12.0.5.0.0
- Oracle Communications Data Model, version 12.2.0.1
- Oracle Communications Design Studio, version 7.4.2
- Oracle Communications Diameter Signaling Router, version 8.6.0.0
- Oracle Communications Element Manager, version 9.0
- Oracle Communications Evolved Communications Application Server, version 7.1
- Oracle Communications Instant Messaging Server, version 10.0.1.6.0
- Oracle Communications Interactive Session Recorder, version 6.4
- Oracle Communications Messaging Server, version 8.1
- Oracle Communications MetaSolv Solution, version 6.3.1
- Oracle Communications Network Charging and Control, versions 6.0.1.0.0, 12.0.1.0.0-12.0.5.0.0
- Oracle Communications Order and Service Management, versions 7.3, 7.4
- Oracle Communications Policy Management, version 12.6.0.0.0
- Oracle Communications Pricing Design Center, versions 12.0.0.4.0-12.0.0.7.0
- Oracle Communications Services Gatekeeper, version 7.0.0.0.0

- Oracle Communications Session Border Controller, versions 8.4, 9.0, 9.1
- Oracle Communications Session Report Manager, version 9.0
- Oracle Communications Unified Assurance, versions prior to 5.5.7.0.0, 6.0.0.0.0
- Oracle Communications User Data Repository, versions 12.4.0, 12.6.0, 12.6.1
- Oracle Communications WebRTC Session Controller, versions 7.2.0, 7.2.1
- Oracle Data Integrator, version 12.2.1.4.0
- Oracle Database Server, versions 19c, 21c
- Oracle Documaker Enterprise Edition, versions 12.6-12.7
- Oracle E-Business Suite, versions 12.2.3-12.2.11
- Oracle Enterprise Data Quality, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle Enterprise Operations Monitor, versions 4.4, 5.0
- Oracle Essbase, version 21.3
- Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.7.0-8.1.0.0, 8.1.1.0, 8.1.2.0, 8.1.2.1
- Oracle Financial Services Behavior Detection Platform, versions 8.0.7.2, 8.0.8.1, 8.1.1.0, 8.1.1.1, 8.1.2.0, 8.1.2.1, 8.1.2.2
- Oracle Financial Services Enterprise Case Management, versions 8.0.7.3, 8.0.8.2, 8.1.1.0, 8.1.1.1, 8.1.2.0, 8.1.2.1, 8.1.2.2
- Oracle Financial Services Model Management and Governance, versions 8.0.8.0, 8.1.0.0, 8.1.1.0
- Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition, versions 8.0.7.0, 8.0.8.0
- Oracle GoldenGate, version 19c
- Oracle GraalVM Enterprise Edition, versions 20.3.7, 21.3.3, 22.2.0
- Oracle Healthcare Data Repository, versions 8.1.1, 8.1.2, 8.1.3
- Oracle Healthcare Foundation, versions 8.1, 8.2
- Oracle Healthcare Master Person Index, versions 5.0.0-5.0.3
- Oracle Healthcare Translational Research, version 4.1
- Oracle Hospitality Cruise Fleet Management System, version 9.1.5
- Oracle Hospitality Cruise Shipboard Property Management System, versions 20.2.0, 20.2.2
- Oracle Hospitality Suite8, versions 8.10.2, 8.11.0, 8.12.0, 8.13.0, 8.14.0
- Oracle HTTP Server, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle Hyperion Infrastructure Technology, version 11.2.9
- Oracle Identity Management Suite, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle Insurance Insbridge Rating and Underwriting, versions 5.2.0, 5.4.0-5.6.2
- Oracle Java SE, versions 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19
- Oracle MapViewer, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle Middleware Common Libraries and Tools, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle NoSQL Database
- Oracle Outside In Technology, version 8.5.6
- Oracle Retail Assortment Planning, version 16.0.3
- Oracle Retail Back Office, version 14.1
- Oracle Retail Central Office, version 14.1

- Oracle Retail Customer Insights, versions 15.0.2, 15.2, 16.0.2
- Oracle Retail Customer Management and Segmentation Foundation, versions 17.0, 18.0, 19.0
- Oracle Retail EFTLink, versions 20.0.1, 21.0.0
- Oracle Retail Fiscal Management, version 14.2
- Oracle Retail Merchandising System, versions 14.1.3.2, 15.0.3.1, 19.0.1
- Oracle Retail Point Of Service, version 14.1
- Oracle Retail Predictive Application Server, versions 14.1.3.47, 15.0.3.116, 16.0.3.260
- Oracle Retail Returns Management, version 14.1
- Oracle Retail Sales Audit, version 19.0.1
- Oracle Retail Service Backbone, versions 14.1.3.2, 15.0.3.1, 16.0.3
- Oracle SD-WAN Aware, version 9.0.1.3.0
- Oracle SD-WAN Edge, versions 7.0.7, 9.1.1.2.0
- Oracle Secure Backup, versions prior to 18.1.0.2.0
- Oracle SOA Suite, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle Solaris, version 11
- Oracle Solaris Cluster, version 4
- Oracle SQL Developer
- Oracle TimesTen In-Memory Database
- Oracle Transportation Management, versions 6.4.3, 6.5.1
- Oracle Utilities Testing Accelerator, versions 6.0.0.1.3, 6.0.0.2.4, 6.0.0.3.3, 7.0.0.0.0
- Oracle VM VirtualBox, versions prior to 6.1.40
- Oracle WebCenter Content, version 12.2.1.3.0
- 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 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0
- PeopleSoft Enterprise Common Components, version 9.2
- PeopleSoft Enterprise PeopleTools, versions 8.58, 8.59, 8.60
- Primavera Gateway, versions 18.8.0-18.8.15, 19.12.0-19.12.14, 20.12.0-20.12.9, 21.12.0-21.12.7
- Primavera Unifier, versions 18.8, 19.12, 20.12, 21.12
- Siebel Applications, versions 22.8 and prior

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 or appropriate mitigations provided by Microsoft to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
- Apply the Principle of Least Privilege to all systems and services, and run all software as a non-privileged user (one without administrative rights) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.
- Remind all users not to visit untrusted websites or follow links/open files provided by unknown or untrusted sources. (**M1017: User Training**)
    - **Safeguard 14.1: Establish and Maintain a Security Awareness Program:** Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks:** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.
- Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior. (**M1040 : Behavior Prevention on Endpoint**)
    - **Safeguard 13.2 : Deploy a Host-Based Intrusion Detection Solution**: Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.
    - **Safeguard 13.7 : Deploy a Host-Based Intrusion Prevention Solution:** Deploy a host-based intrusion prevention solution on enterprise assets, where

appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

REFERENCES:

Oracle:

https://www.oracle.com/security-alerts/cpuoct2022.html