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:
07/20/2021

SUBJECT:
Oracle Quarterly Critical Patches Issued July 20, 2021

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

SYSTEMS AFFECTED:
- Oracle Database Server, versions 12.1.0.2, 19c
- Big Data Spatial and Graph, versions prior to 2.0, prior to 23.1
- Essbase, version 21.2
- Essbase Analytic Provider Services, versions 11.1.2.4, 21.2
- Hyperion Essbase Administration Services, versions 11.1.2.4, 21.2
- Oracle Commerce Guided Search / Oracle Commerce Experience Manager, version 11.3.1.5
- Oracle Communications Billing and Revenue Management, versions 7.5.0.23.0, 12.0.0.3.0
- Oracle Communications BRM - Elastic Charging Engine, versions 11.3.0.9.0, 12.0.0.3.0
- Oracle Communications Convergent Charging Controller, version 12.0.4.0.0
- Oracle Communications Design Studio, version 7.4.2
- Oracle Communications Instant Messaging Server, version 10.0.1.4.0
- Oracle Communications Network Charging and Control, versions 6.0.1.0, 12.0.1.0-12.0.4.0, 12.0.4.0.0
- Oracle Communications Offline Mediation Controller, version 12.0.0.3.0
- Oracle Communications Pricing Design Center, version 12.0.0.3.0
- Oracle Communications Unified Inventory Management, versions 7.3.2, 7.3.4, 7.3.5, 7.4.0, 7.4.1
- Oracle Communications Application Session Controller, version 3.9
- Oracle Communications Cloud Native Core Console, version 1.4.0
- Oracle Communications Cloud Native Core Network Function Cloud Native Environment, versions 1.4.0, 1.7.0
- Oracle Communications Cloud Native Core Network Slice Selection Function, version 1.2.1
- Oracle Communications Cloud Native Core Policy, versions 1.5.0, 1.9.0

- Oracle Communications Cloud Native Core Security Edge Protection Proxy, version 1.7.0
- Oracle Communications Cloud Native Core Service Communication Proxy, version 1.5.2
- Oracle Communications Cloud Native Core Unified Data Repository, versions 1.4.0, 1.6.0
- Oracle Communications Diameter Signaling Router (DSR), versions 8.0.0-8.5.0
- Oracle Communications EAGLE Software, versions 46.6.0-46.8.2
- Oracle Communications Evolved Communications Application Server, version 7.1
- Oracle Communications Services Gatekeeper, versions 7.0, 8.2
- Instantis EnterpriseTrack, versions 17.1, 17.2, 17.3
- Primavera Gateway, versions 17.12.0-17.12.11, 18.8.0-18.8.11, 19.12.0-19.12.10, 20.12.0
- Primavera P6 Enterprise Project Portfolio Management, versions 17.12.0-17.12.20, 18.8.0-18.8.23, 19.12.0-19.12.14, 20.12.0-20.12.3
- Primavera Unifier, versions 17.7-17.12, 18.8, 19.12, 20.12
- Oracle E-Business Suite, versions 12.1.1-12.1.3, 12.2.3-12.2.10
- Enterprise Manager Base Platform, version 13.4.0.0
- Oracle Application Testing Suite, version 13.3.0.1
- Oracle Configuration Manager, version 12.1.2.0.8
- Oracle Banking Enterprise Collections, versions 2.10.0, 2.12.0
- Oracle Banking Party Management, version 2.7.0
- Oracle Banking Platform, versions 2.4.0, 2.7.1, 2.9.0
- Oracle Banking Treasury Management, version 14.4
- Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.6-8.0.9, 8.1.0
- Oracle Financial Services Crime and Compliance Investigation Hub, version 20.1.2
- Oracle Financial Services Regulatory Reporting with AgileREPORTER, version 8.0.9.6.3
- Oracle FLEXCUBE Private Banking, versions 12.0.0, 12.1.0
- Oracle FLEXCUBE Universal Banking, versions 12.0-12.4, 14.0-14.4.0
- MICROS Compact Workstation 3, version 310
- MICROS ES400 Series, versions 400-410
- MICROS Kitchen Display System Hardware, version 210
- MICROS Workstation 5A, version 5A
- MICROS Workstation 6, versions 610-655
- Oracle Hospitality Reporting and Analytics, version 9.1.0
- Identity Manager, versions 11.1.2.2.0, 11.1.2.3.0, 12.2.1.3.0, 12.2.1.4.0
- Oracle Access Manager, version 11.1.2.3.0
- Oracle BAM (Business Activity Monitoring), versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0
- Oracle BI Publisher, versions 5.5.0.0.0, 11.1.1.7.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0
- Oracle Business Intelligence Enterprise Edition, version 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 Data Integrator, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle Enterprise Data Quality, version 12.2.1.3.0
- Oracle Enterprise Repository, version 11.1.1.7.0
- Oracle Fusion Middleware MapViewer, version 12.2.1.4.0
- Oracle GoldenGate Application Adapters, version 19.1.0.0.0
- Oracle JDeveloper, version 12.2.1.4.0
- Oracle JDeveloper and ADF, version 12.2.1.4.0

- Oracle Managed File Transfer, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle Outside In Technology, version 8.5.5
- Oracle WebCenter Portal, versions 11.1.1.9.0, 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
- Real-Time Decisions (RTD) Solutions, version 3.2.0.0
- Oracle Hospitality Suite8, versions 8.13, 8.14
- Hyperion Financial Reporting, versions 11.1.2.4, 11.2.5.0
- Hyperion Infrastructure Technology, versions 11.1.2.4, 11.2.5.0
- Oracle Hyperion BI+, versions 11.1.2.4, 11.2.5.0
- Oracle Insurance Policy Administration, versions 11.0.2, 11.1.0-11.3.0
- Oracle Insurance Policy Administration J2EE, version 11.0.2
- Oracle Insurance Rules Palette, versions 11.0.2, 11.1.0-11.3.0
- Oracle GraalVM Enterprise Edition, versions 20.3.2, 21.1.0
- Oracle Java SE, versions 7u301, 8u291, 11.0.11, 16.0.1
- JD Edwards EnterpriseOne Orchestrator, versions 9.2.5.3 and prior
- JD Edwards EnterpriseOne Tools, versions 9.2.5.3 and prior
- MySQL Cluster, versions 8.0.25 and prior
- MySQL Connectors, versions 8.0.23 and prior
- MySQL Enterprise Monitor, versions 8.0.23 and prior
- MySQL Server, versions 5.7.34 and prior, 8.0.25 and prior
- PeopleSoft Enterprise CS Campus Community, version 9.2
- PeopleSoft Enterprise HCM Candidate Gateway, version 9.2
- PeopleSoft Enterprise HCM Shared Components, version 9.2
- PeopleSoft Enterprise PeopleTools, versions 8.57, 8.58, 8.59
- PeopleSoft Enterprise PT PeopleTools, versions 8.57, 8.58, 8.59
- Oracle Policy Automation, versions 12.2.0-12.2.22
- Oracle Retail Back Office, version 14.1
- Oracle Retail Central Office, version 14.1
- Oracle Retail Customer Engagement, versions 16.0-19.0
- Oracle Retail Customer Management and Segmentation Foundation, versions 16.0-19.0
- Oracle Retail Financial Integration, versions 14.1.3.2, 15.0.3.1, 16.0.3.0
- Oracle Retail Integration Bus, versions 14.1.3.2, 15.0.3.1, 16.0.3.0
- Oracle Retail Merchandising System, versions 14.1.3.2, 15.0.3.1, 16.0.3
- Oracle Retail Order Broker, versions 15.0, 16.0
- Oracle Retail Order Management System Cloud Service, version 19.5
- Oracle Retail Point-of-Service, version 14.1
- Oracle Retail Price Management, versions 14.0, 14.1, 15.0, 16.0
- Oracle Retail Returns Management, version 14.1
- Oracle Retail Service Backbone, versions 14.1.3.2, 15.0.3.1, 16.0.3.0
- Oracle Retail Xstore Point of Service, versions 16.0.6, 17.0.4, 18.0.3, 19.0.2, 20.0.1
- Siebel Applications, versions 21.5 and prior
- Oracle Agile Engineering Data Management, version 6.2.1.0
- Oracle Agile PLM, versions 9.3.3, 9.3.5, 9.3.6
- Oracle Transportation Management, version 6.4.3
- OSS Support Tools, versions prior to 2.12.41
- Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers, versions prior to XCP2400, prior to XCP3100

- Oracle Solaris, version 11
- Oracle Solaris Cluster, version 4.4
- Oracle ZFS Storage Appliance Kit, version 8.8
- StorageTek Tape Analytics SW Tool, version 2.3
- Oracle Secure Global Desktop, version 5.6
- Oracle VM VirtualBox, versions prior to 6.1.24

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 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:
Oracle:
https://www.oracle.com/security-alerts/cpujul2021.html

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.