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:
04/19/2022
04/22/2022 - UPDATED

SUBJECT:
Oracle Quarterly Critical Patches Issued April 19, 2022

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

April 22 – THREAT INTELLIGENCE UPDATED:

A new proof of concept code demonstrating a newly disclosed digital signature bypass vulnerability in Java has been shared online. The high-severity flaw in question, CVE-2022-21449 (CVSS score: 7.5), impacts the following version of Java SE and Oracle GraalVM Enterprise Edition:

- ***Oracle Java SE, versions 7u331, 8u321, 11.0.14, 17.0.2, 18***
- ***Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1, 22.0.0.2***

The issue resides in Java's implementation of the Elliptic Curve Digital Signature Algorithm (ECDSA), a cryptographic mechanism to digitally sign messages and data for verifying the authenticity and the integrity of the contents. The cryptographic vulnerability in Java makes it possible to present a totally blank signature, which would still be perceived as valid by the vulnerable implementation.

SYSTEMS AFFECTED:

- Engineered Systems Utilities, versions 12.1.0.2, 19c, 21c
- Enterprise Manager Base Platform, versions 13.4.0.0, 13.5.0.0
- Enterprise Manager for Peoplesoft, versions 13.4.1.1, 13.5.1.1
- Enterprise Manager for Storage Management, version 13.4.0.0
- Enterprise Manager Ops Center, version 12.4.0.0

- Helidon, versions 1.4.7, 1.4.10, 2.0.0-RC1
- Instantis EnterpriseTrack, versions 17.1, 17.2, 17.3
- JD Edwards EnterpriseOne Tools, versions prior to 9.2.6.3
- JD Edwards World Security, version A9.4
- Management Cloud Engine, versions 1.5.0 and prior
- Middleware Common Libraries and Tools, versions 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0
- MySQL Cluster, versions 7.4.35 and prior, 7.5.25 and prior, 7.6.21 and prior, 8.0.28 and prior
- MySQL Connectors, versions 8.0.28 and prior
- MySQL Enterprise Monitor, versions 8.0.29 and prior
- MySQL Server, versions 5.7.37 and prior, 8.0.28 and prior
- MySQL Workbench, versions 8.0.28 and prior
- Oracle Advanced Supply Chain Planning, versions 12.1, 12.2
- Oracle Agile Engineering Data Management, version 6.2.1.0
- Oracle Agile PLM, version 9.3.6
- Oracle Agile PLM MCAD Connector, version 3.6
- Oracle Application Express, versions prior to 22.1
- Oracle Application Testing Suite, version 13.3.0.1
- Oracle Autovue for Agile Product Lifecycle Management, version 21.0.2
- Oracle Banking Deposits and Lines of Credit Servicing, version 2.12.0
- Oracle Banking Enterprise Default Management, versions 2.7.1, 2.10.0, 2.12.0
- Oracle Banking Loans Servicing, version 2.12.0
- Oracle Banking Party Management, version 2.7.0
- Oracle Banking Payments, version 14.5
- Oracle Banking Platform, versions 2.6.2, 2.7.1, 2.12.0
- Oracle Banking Trade Finance, version 14.5
- Oracle Banking Treasury Management, version 14.5
- Oracle Blockchain Platform, versions prior to 21.1.2
- Oracle Business Intelligence Enterprise Edition, versions 5.5.0.0.0, 5.9.0.0.0, 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 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0
- Oracle Commerce Guided Search, version 11.3.2
- Oracle Communications ASAP, version 7.3
- Oracle Communications Billing and Revenue Management, versions 12.0.0.4, 12.0.0.5
- Oracle Communications Cloud Native Core Automated Test Suite, versions 1.8.0, 1.9.0, 22.1.0
- Oracle Communications Cloud Native Core Binding Support Function, version 1.11.0
- Oracle Communications Cloud Native Core Console, versions 1.9.0, 22.1.0
- Oracle Communications Cloud Native Core Network Exposure Function, version 22.1.0
- Oracle Communications Cloud Native Core Network Function Cloud Native Environment, versions 1.10.0, 22.1.0
- Oracle Communications Cloud Native Core Network Repository Function, versions 1.15.0, 1.15.1, 22.1.0

- Oracle Communications Cloud Native Core Network Slice Selection Function, versions 1.8.0, 22.1.0
- Oracle Communications Cloud Native Core Policy, versions 1.14.0, 1.15.0, 22.1.0
- Oracle Communications Cloud Native Core Security Edge Protection Proxy, versions 1.7.0, 22.1.0
- Oracle Communications Cloud Native Core Service Communication Proxy, version 1.15.0
- Oracle Communications Cloud Native Core Unified Data Repository, versions 1.15.0, 22.1.0
- Oracle Communications Contacts Server, version 8.0.0.6.0
- Oracle Communications Convergence, versions 3.0.2.2, 3.0.3.0
- Oracle Communications Convergent Charging Controller, versions 6.0.1.0.0, 12.0.1.0.0-12.0.4.0.0
- Oracle Communications Design Studio, versions 7.3.5, 7.4.0-7.4.2
- Oracle Communications Diameter Intelligence Hub, versions 8.0.0-8.2.3
- Oracle Communications Diameter Signaling Router, version 8.4.0.0
- Oracle Communications EAGLE Application Processor
- Oracle Communications EAGLE Element Management System, version 46.6
- Oracle Communications EAGLE FTP Table Base Retrieval, version 4.5
- Oracle Communications EAGLE LNP Application Processor, versions 10.1, 10.2
- Oracle Communications EAGLE Software, versions 46.7.0, 46.8.0-46.8.2, 46.9.1-46.9.3
- Oracle Communications Element Manager, versions prior to 9.0
- Oracle Communications Evolved Communications Application Server, version 7.1
- Oracle Communications Instant Messaging Server, version 10.0.1.5.0
- Oracle Communications Interactive Session Recorder, version 6.4
- Oracle Communications IP Service Activator, version 7.4.0
- 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, 12.0.1.0.0-12.0.4.0.0
- Oracle Communications Network Integrity, versions 7.3.2, 7.3.5, 7.3.6
- Oracle Communications Operations Monitor, versions 4.3, 4.4, 5.0
- Oracle Communications Order and Service Management, versions 7.3, 7.4
- Oracle Communications Performance Intelligence Center (PIC) Software, versions 10.3.0.0.0-10.3.0.2.1, 10.4.0.1.0-10.4.0.3.1
- Oracle Communications Policy Management, versions 12.5.0.0.0, 12.6.0.0.0
- Oracle Communications Pricing Design Center, versions 12.0.0.4, 12.0.0.5
- Oracle Communications Services Gatekeeper, version 7.0.0.0.0
- Oracle Communications Session Border Controller, versions 8.4, 9.0
- Oracle Communications Session Report Manager, versions prior to 9.0
- Oracle Communications Session Route Manager, versions prior to 9.0
- Oracle Communications Unified Inventory Management, versions 7.4.1, 7.4.2
- Oracle Communications Unified Session Manager, versions 8.2.5, 8.4.5
- Oracle Communications User Data Repository, version 12.4

- Oracle Communications WebRTC Session Controller, version 7.2.1
- Oracle Data Integrator, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle Database Server, versions 12.1.0.2, 19c, 21c
- Oracle Documaker, versions 12.6.0, 12.6.2-12.6.4, 12.7.0
- Oracle E-Business Suite, versions 12.2.4-12.2.11, [EBS Cloud Manager and Backup Module] prior to 22.1.1.1, [Enterprise Command Center] 7.0, [Enterprise Information Discovery] 7-9
- Oracle Enterprise Communications Broker, versions 3.2, 3.3
- Oracle Enterprise Session Border Controller, versions 8.4, 9.0
- Oracle Ethernet Switch ES1-24, version 1.3.1
- Oracle Ethernet Switch TOR-72, version 1.2.2
- Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.6.0-8.0.9.0, 8.1.0.0-8.1.2.0
- Oracle Financial Services Behavior Detection Platform, versions 8.0.6.0-8.0.8.0, 8.1.1.0, 8.1.1.1, 8.1.2.0
- Oracle Financial Services Enterprise Case Management, versions 8.0.7.1, 8.0.7.2, 8.0.8.0, 8.0.8.1, 8.1.1.0, 8.1.1.1, 8.1.2.0
- Oracle Financial Services Revenue Management and Billing, versions 2.7.0.0, 2.7.0.1, 2.8.0.0
- Oracle FLEXCUBE Universal Banking, versions 11.83.3, 12.1-12.4, 14.0-14.3, 14.5
- Oracle Global Lifecycle Management OPatch
- Oracle GoldenGate, versions prior to 12.3.0.1.2, prior to 23.1
- Oracle GoldenGate Application Adapters, versions prior to 23.1
- Oracle GoldenGate Big Data and Application Adapters, versions prior to 23.1
- Oracle GraalVM Enterprise Edition, versions 20.3.5, 21.3.1, 22.0.0.2
- Oracle Health Sciences Empirica Signal, versions 9.1.0.6, 9.2.0.0
- Oracle Health Sciences InForm, versions 6.2.1.1, 6.3.2.1, 7.0.0.0
- Oracle Health Sciences InForm Publisher, versions 6.2.1.1, 6.3.1.1
- Oracle Health Sciences Information Manager, versions 3.0.1-3.0.4
- Oracle Healthcare Data Repository, versions 8.1.0, 8.1.1
- Oracle Healthcare Foundation, versions 7.3.0.1-7.3.0.4
- Oracle Healthcare Master Person Index, version 5.0.1
- Oracle Healthcare Translational Research, versions 4.1.0, 4.1.1
- Oracle Hospitality Suite8, versions 8.10.2, 8.11.0-8.14.0
- Oracle Hospitality Token Proxy Service, version 19.2
- Oracle HTTP Server, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle Hyperion BI+, versions prior to 11.2.8.0
- Oracle Hyperion Calculation Manager, versions prior to 11.2.8.0
- Oracle Hyperion Data Relationship Management, versions prior to 11.2.8.0, prior to 11.2.9.0
- Oracle Hyperion Financial Management, versions prior to 11.2.8.0
- Oracle Hyperion Infrastructure Technology, versions prior to 11.2.8.0
- Oracle Hyperion Planning, versions prior to 11.2.8.0
- Oracle Hyperion Profitability and Cost Management, versions prior to 11.2.8.0

- Oracle Hyperion Tax Provision, versions prior to 11.2.8.0
- Oracle Identity Management Suite, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle Identity Manager Connector, versions 9.1.0, 11.1.1.5.0
- Oracle iLearning, versions 6.2, 6.3
- Oracle Insurance Data Gateway, version 1.0.1
- Oracle Insurance Insbridge Rating and Underwriting, versions 5.2.0, 5.4.0-5.6.0, 5.6.1
- Oracle Insurance Policy Administration, versions 11.0.2, 11.1.0, 11.2.8, 11.3.0, 11.3.1
- Oracle Insurance Rules Palette, versions 11.0.2, 11.1.0, 11.2.8, 11.3.0, 11.3.1
- Oracle Internet Directory, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle Java SE, versions 7u331, 8u321, 11.0.14, 17.0.2, 18
- Oracle JDeveloper, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle Managed File Transfer, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle Middleware Common Libraries and Tools, version 12.2.1.4.0
- Oracle NoSQL Database
- Oracle Outside In Technology, version 8.5.5
- Oracle Payment Interface, versions 19.1, 20.3
- Oracle Product Lifecycle Analytics, version 3.6.1.0
- Oracle REST Data Services, versions prior to 21.2
- Oracle Retail Bulk Data Integration, version 16.0.3
- Oracle Retail Customer Insights, versions 15.0.2, 16.0.2
- Oracle Retail Customer Management and Segmentation Foundation, versions 17.0-19.0
- Oracle Retail Data Extractor for Merchandising, versions 15.0.2, 16.0.2
- Oracle Retail EFTLink, versions 17.0.2, 18.0.1, 19.0.1, 20.0.1, 21.0.0
- Oracle Retail Extract Transform and Load, version 13.2.8
- Oracle Retail Financial Integration, versions 14.1.3.2, 15.0.3.1, 16.0.1-16.0.3, 19.0.0, 19.0.1
- Oracle Retail Integration Bus, versions 14.1.3.2, 15.0.3.1, 16.0.1-16.0.3, 19.0.0, 19.0.1
- Oracle Retail Invoice Matching, version 16.0.3
- Oracle Retail Merchandising System, versions 16.0.3, 19.0.1
- Oracle Retail Service Backbone, versions 14.1.3.2, 15.0.3.1, 16.0.1-16.0.3, 19.0.0, 19.0.1
- Oracle Retail Store Inventory Management, versions 14.0.4.13, 14.1.3.5, 14.1.3.14, 15.0.3.3, 15.0.3.8, 16.0.3.7
- Oracle Retail Xstore Office Cloud Service, versions 16.0.6, 17.0.4, 18.0.3, 19.0.2, 20.0.1
- Oracle Retail Xstore Point of Service, versions 16.0.6, 17.0.4, 18.0.3, 19.0.2, 20.0.1, 21.0.0
- Oracle SD-WAN Edge, versions 9.0, 9.1
- Oracle Secure Backup
- Oracle Secure Global Desktop, version 5.6
- Oracle Solaris, version 11
- Oracle Solaris Cluster, version 4
- Oracle SQL Developer, versions prior to 21.99
- Oracle StorageTek ACSLS, version 8.5.1

- Oracle StorageTek Tape Analytics (STA), version 2.4
- Oracle Taleo Platform, versions prior to 22.1
- Oracle Transportation Management, versions 6.4.3, 6.5.1
- Oracle Tuxedo, version 12.2.2.0.0
- Oracle Utilities Framework, versions 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 6.1.34
- Oracle Web Services Manager, versions 12.2.1.3.0, 12.2.1.4.0
- 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
- Oracle ZFS Storage Appliance Kit, version 8.8
- OSS Support Tools, versions 2.12.42, 18.3
- PeopleSoft Enterprise CS Academic Advisement, version 9.2
- PeopleSoft Enterprise FIN Cash Management, version 9.2
- PeopleSoft Enterprise PeopleTools, versions 8.58, 8.59
- PeopleSoft Enterprise PRTL Interaction Hub, version 9.1
- Primavera Unifier, versions 17.7-17.12, 18.8, 19.12, 20.12, 21.12

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 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.

April 22 – UPDATED RECOMMENDATIONS:
We recommend updating to your latest version of Java as soon as possible (Versions 17.0.3 and 18.0.1)

REFERENCES:

Oracle:
https://www.oracle.com/security-alerts/cpuapr2022.html

April 22 – UPDATED REFERENCES:
Oracle Latest Java Version Download:
https://www.oracle.com/java/technologies/downloads/

TheHackerNews:
https://thehackernews.com/2022/04/researcher-releases-poc-for-recent-java.html