January 18, 2024

Overall rating: Critical

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Oracle published a security advisory to address vulnerabilities in multiple products. Included were critical updates for the following:

- Oracle Communications Applications
- Oracle Communications
- Oracle Essbase
- Oracle Financial Services
- Oracle Fusion Middleware
- Oracle Hyperion
- Oracle JD Edwards
- Oracle MySQL
- Oracle REST Data Services
- Oracle Retail Applications
- Oracle Secure Backup
- Oracle SQL Developer
- Oracle Systems
- Oracle TimesTen In-Memory Database

Technical Details

A Critical Patch Update is a collection of patches for multiple security vulnerabilities. These patches address vulnerabilities in Oracle code and in third party components included in Oracle products. These patches are usually cumulative, but each advisory describes only the security patches added since the previous Critical Patch Update Advisory. Thus, prior Critical Patch Update advisories should be reviewed for information regarding earlier published security patches. Refer to “Critical Patch Updates, Security Alerts and Bulletins” for information about Oracle Security advisories.
Updated products:

CVE-2024-20903	Java VM	6.5
CVE-2023-38545	Oracle Spatial and Graph (curl)	6.5
CVE-2022-21432	Oracle Text	2.7
CVE-2024-20924	Oracle Audit Vault and Database Firewall	7.6
CVE-2024-20909	Oracle Audit Vault and Database Firewall	7.5
CVE-2024-20910	Oracle Audit Vault and Database Firewall	3
CVE-2024-20912	Oracle Audit Vault and Database Firewall	2.7
CVE-2023-46589	Oracle Big Data Spatial and Graph	7.5
CVE-2023-38545	Oracle Essbase	9.8

CVE-2022-3602	Oracle Essbase	7.5
CVE-2023-42503	Oracle Essbase	5.5
CVE-2023-5072	Oracle GoldenGate	3.7
CVE-2023-46589	Graph Server and ClientPackaging (Apache Tomcat)HTTPYes	7.5
CVE-2023-34462-	Oracle NoSQL DatabaseAdministration (Netty)TLSNo	6.5

These vulnerabilities are rated as an overall **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- Oracle Critical Patch Update Advisory – January 2024