October 20, 2023

Overall rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of Oracle's critical patch update. 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.

Technical Details

This Critical Patch Update contains 387 new security patches across the product families listed below.

Affected Products and Versions	Patch Availability Document
BI Publisher, versions 6.4.0.0.0, 7.0.0.0.0, 12.2.1.4.0	Oracle Analytics
GoldenGate Big Data, versions 21.3-21.10	Database
GoldenGate Veridata, versions 12.2.1.4.0-12.2.1.4.230922	Database
Hospitality OPERA 5 Property Services, version 5.6	Oracle Hospitality OPERA 5 Property Services
JD Edwards EnterpriseOne Tools, version 9.2.7	JD Edwards
Management Cloud Engine, version 23.1.0.0	Management Cloud Engine
MySQL Cluster, versions 8.0.34 and prior, 8.1.0	MySQL
MySQL Connectors, versions 8.1.0 and prior	MySQL
MySQL Enterprise Monitor, versions 8.0.35 and prior	MySQL
MySQL Installer, versions prior to 1.6.8	MySQL
MySQL Server, versions 5.7.43 and prior, 8.0.34 and prior, 8.1.0 and prior	MySQL
MySQL Shell, versions 8.1.1 and prior	MySQL
Oracle Access Manager, version 12.2.1.4.0	Fusion Middleware
Oracle Agile PLM, version 9.3.6	Oracle Supply Chain Products
Oracle Application Testing Suite, version 13.3.0.1	Oracle Enterprise Manager
Oracle Banking APIs, versions 18.3, 19.1, 19.2, 21.1, 22.1, 22.2	Contact Support
Oracle Banking Branch, versions 14.5-14.7	Contact Support
Oracle Banking Cash Management, versions 14.5-14.7	Contact Support
Oracle Banking Corporate Lending, versions 14.0-14.3, 14.5-14.7	Contact Support
Oracle Banking Corporate Lending Process Management, versions 14.5-14.7	Contact Support
Oracle Banking Credit Facilities Process Management, versions 14.5-14.7	Contact Support
Oracle Banking Deposits and Lines of Credit Servicing, versions 2.7, 2.12	Contact Support
Oracle Banking Digital Experience, versions 18.3, 19.1, 19.2, 21.1, 22.1, 22.2	Contact Support
Oracle Banking Electronic Data Exchange for Corporates, versions 14.5-14.7	Contact Support
Oracle Banking Liquidity Management, versions 14.5-14.7	Contact Support
Oracle Banking Loans Servicing, version 2.12	Oracle Banking Platform
Oracle Banking Origination, versions 14.5-14.7	Contact Support
Oracle Banking Party Management, version 2.7	Oracle Banking Platform
Oracle Banking Payments, versions 14.0-14.3, 14.5-14.7	Contact Support
Oracle Banking Platform, versions 2.6.2, 2.9.0	Oracle Banking Platform
Oracle Banking Supply Chain Finance, versions 14.5-14.7	Contact Support

Oracle Banking Trade Finance, versions 14.5-14.7	Contact Support
Oracle Banking Trade Finance Process Management, versions 14.5-14.7	Contact Support
Oracle Banking Virtual Account Management, versions 14.5-14.7	Contact Support
Oracle Big Data Spatial and Graph, versions 2.5 and prior	Database
Oracle Business Intelligence Enterprise Edition, versions 6.4.0.0.0, 7.0.0.0.0, 12.2.1.4.0	Oracle Analytics
Oracle Business Process Management Suite, version 12.2.1.4.0	Fusion Middleware
Oracle Coherence, versions 12.2.1.4.0, 14.1.1.0.0	Fusion Middleware
Oracle Commerce Guided Search, version 11.3.2	Oracle Commerce
Oracle Communications BRM - Elastic Charging Engine, versions 12.0.0.4-12.0.0.8	Oracle Communications BRM - Elastic Charging Engine
Oracle Communications Cloud Native Core Binding Support Function, versions 23.1.0-23.1.8, 23.2.0-23.2.4	Oracle Communications Cloud Native Core Binding Support Function
Oracle Communications Cloud Native Core Console, versions 23.1.1, 23.1.2, 23.2.1	Oracle Communications Cloud Native Core Console
Oracle Communications Cloud Native Core Network Exposure Function, versions 23.1.3, 23.3.0	Oracle Communications Cloud Native Core Network Exposure Function
Oracle Communications Cloud Native Core Network Function Cloud Native Environment, versions 23.2.0, 23.2.2	Oracle Communications Cloud Native Core Network Function Cloud Native Environment
Oracle Communications Cloud Native Core Network Repository Function, versions 23.1.3, 23.2.1, 23.3.0	Oracle Communications Cloud Native Core Network Repository Function
Oracle Communications Cloud Native Core Policy, versions 23.1.0-23.1.8, 23.2.0-23.2.4	Oracle Communications Cloud Native Core Policy
Oracle Communications Cloud Native Core Security Edge Protection Proxy, versions 23.1.0, 23.1.3, 23.3.0	Oracle Communications Cloud Native Core Security Edge Protection Proxy
Oracle Communications Cloud Native Core Unified Data Repository, version 23.1.2	Oracle Communications Cloud Native Core Unified Data Repository
Oracle Communications Convergent Charging Controller, version 12.0.6.0	Oracle Communications Convergent Charging Controller
Oracle Communications Diameter Signaling Router, versions 8.6.0.0, 9.0.0.0	Oracle Communications Diameter Signaling Router
Oracle Communications Element Manager, versions 9.0.0-9.0.2	Oracle Communications Element Manager
Oracle Communications IP Service Activator, versions 7.4.0, 7.5.0	Oracle Communications IP Service Activator
Oracle Communications MetaSolv Solution, version 6.3.1.0.0	Oracle Communications MetaSolv Solution
Oracle Communications Network Analytics Data Director, version 23.2.0	Oracle Communications Network Analytics Data Director
Oracle Communications Network Charging and Control, version 12.0.6.0	Oracle Communications Network Charging and Control
Oracle Communications Order and Service Management, versions 7.4.0, 7.4.1	Oracle Communications Order and Service Management
Oracle Communications Policy Management, version 12.6.0.0	Oracle Communications Policy Management
Oracle Communications Session Report Manager, versions 9.0.0-9.0.2	Oracle Communications Session Report Manager
Oracle Communications Unified Assurance, versions 5.5.0-5.5.17, 6.0.0-6.0.3	Oracle Communications Unified Assurance
Oracle Communications WebRTC Session Controller, versions 7.2.0.0.0, 7.2.1.0.0	Oracle Communications WebRTC Session Controller
Oracle Data Integrator, version 12.2.1.4.0	Fusion Middleware
Oracle Database Server, versions 19.3-19.20, 21.3-21.11	Database

Oracle Documaker, versions 12.6.4-12.7.1	Oracle Insurance Applications
Oracle E-Business Suite, versions 12.2.3-12.2.12, [ECC] 8, [ECC] 9, [ECC] 10	Oracle E-Business Suite
Oracle Enterprise Communications Broker, versions 3.3, 4.0, 4.1	Oracle Enterprise Communications Broker
Oracle Enterprise Data Quality, version 12.2.1.4.0	Fusion Middleware
Oracle Enterprise Manager Base Platform, version 13.5.0.0	Oracle Enterprise Manager
Oracle Enterprise Manager for Peoplesoft, version 13.5.1.1	Oracle Enterprise Manager
Oracle Enterprise Manager Ops Center, version 12.4.0.0	Oracle Enterprise Manager
Oracle Enterprise Operations Monitor, versions 5.0, 5.1	Oracle Enterprise Operations Monitor
Oracle Enterprise Session Border Controller, versions 9.0-9.2	Oracle Enterprise Session Border Controller
Oracle Essbase, version 21.5.0.0.0	Database
Oracle Financial Services Cash Flow Engine, version 8.1.2.0.0	Contact Support
Oracle Financial Services Model Management and Governance, versions 8.1.2.3, 8.1.2.4	Oracle Financial Services Model Management and Governance
Oracle FLEXCUBE Core Banking, versions 11.6-11.8, 11.10, 11.11	Contact Support
Oracle FLEXCUBE Enterprise Limits and Collateral Management, versions 12.3, 12.4, 14.0-14.3, 14.5-14.7	Contact Support
Oracle FLEXCUBE Universal Banking, versions 12.3, 12.4, 14.0-14.3, 14.5-14.7	Contact Support
Oracle Fusion Middleware MapViewer, version 12.2.1.4.0	Fusion Middleware
Oracle Global Lifecycle Management OPatch, versions prior to 12.2.0.1.40	Global Lifecycle Management
Oracle GoldenGate Studio, version 12.2.1.4.0	Database
Oracle GraalVM for JDK, versions 17.0.8, 21	Java SE
Oracle Graph Server and Client, versions 22.4.4 and prior	Database
Oracle Healthcare Master Person Index, versions 5.0.0-5.0.6	HealthCare Applications
Oracle HTTP Server, version 12.2.1.4.0	Fusion Middleware
Oracle Hyperion Infrastructure Technology, version 11.2.14.0.0	Oracle Enterprise Performance Management
Oracle Identity Manager, version 12.2.1.4.0	Fusion Middleware
Oracle Java SE, versions 8u381, 8u381-perf, 11.0.20, 17.0.8, 21	Java SE
Oracle Life Sciences InForm, version 7.0.0.0	Health Sciences
Oracle Life Sciences InForm Publisher, version 6.3.1.0	Health Sciences
Oracle Managed File Transfer, version 12.2.1.4.0	Fusion Middleware
Oracle Middleware Common Libraries and Tools, version 12.2.1.4.0	Fusion Middleware
Oracle Outside In Technology, version 8.5.6	Fusion Middleware
Oracle REST Data Services, versions prior to 23.2.2	Database
Oracle Retail Bulk Data Integration, versions 16.0.3, 19.0.1	Retail Applications
Oracle Retail Customer Management and Segmentation Foundation, versions 18.0.0.13, 19.0.0.7	Retail Applications
Oracle Retail EFTLink, versions 20.0.1, 21.0.0, 22.0.0	Retail Applications
Oracle Retail Financial Integration, versions 14.1.3.2, 15.0.3.1, 16.0.3, 19.0.1	Retail Applications
Oracle Retail Fiscal Management, version 14.2	Retail Applications
Oracle Retail Integration Bus, versions 14.1.3.2, 15.0.3.1, 16.0.3, 19.0.1	Retail Applications
Oracle Retail Merchandising System, version 19.0.1	Retail Applications
Oracle Retail Service Backbone, versions 14.1.3.2, 15.0.3.1, 16.0.3, 19.0.1	Retail Applications
Oracle Retail Xstore Point of Service, versions 18.0.5, 19.0.4, 20.0.3, 21.0.2, 22.0.0	Retail Applications
Oracle SD-WAN Edge, versions 9.1.1.5.0, 9.1.1.6.0	Oracle SD-WAN Edge
Oracle Secure Backup, versions 18.1.0.1.0, 18.1.0.2.0	Oracle Secure Backup
Oracle Service Bus, version 12.2.1.4.0	Fusion Middleware
Oracle SOA Suite, version 12.2.1.4.0	Fusion Middleware
Oracle Solaris, versions 10, 11	Systems
Oracle Unified Directory, version 12.2.1.4.0	Fusion Middleware

Oracle Utilities Application Framework, versions 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, 4.5.0.0.0, 4.5.0.0.1, 4.5.0.1.0-4.5.0.1.2	Oracle Utilities Applications
Oracle Utilities Network Management System, versions 2.3.0.2, 2.4.0.1	Oracle Utilities Applications
Oracle VM VirtualBox, versions prior to 7.0.12	Virtualization
Oracle WebCenter Content, version 12.2.1.4.0	Fusion Middleware
Oracle WebCenter Portal, version 12.2.1.4.0	Fusion Middleware
Oracle WebLogic Server, versions 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0	Fusion Middleware
PeopleSoft Enterprise CC Common Application Objects, version 9.2	PeopleSoft
PeopleSoft Enterprise HCM Global Payroll Switzerland, version 9.2	PeopleSoft
PeopleSoft Enterprise PeopleTools, versions 8.59, 8.60	PeopleSoft
Primavera Gateway, versions 19.12.0-19.12.17, 20.12.0-20.12.12, 21.12.0-21.12.10	Oracle Construction and Engineering Suite
Primavera Unifier, versions 19.12.0-19.12.16, 20.12.0-20.12.16, 21.12.0-21.12.16, 22.12.0-22.12.9	Oracle Construction and Engineering Suite
Siebel Applications, versions 23.8 and prior	Siebel
Sun ZFS Storage Appliance, version 8.8.60	Systems
TimesTen In-Memory Database, versions prior to 18.1.4.38.0, prior to 18.1.4.39.0, prior to 22.1.1.18.0	Database

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

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

References

- CVE-2023-22946, CVE-2022-1471, CVE-2022-26612, CVE-2022-29599, CVE-2022-36944, CVE-2022-42920, CVE-2023-20873, CVE-2023-22069, CVE-2023-22072, CVE-2023-22089, CVE-2023-25690, CVE-2023-34034, CVE-2023-3824, CVE-2023-38408, CVE-2023-39017, CVE-2023-39022, CVE-2023-23914, CVE-2022-24834, CVE-2022-42898, CVE-2023-22085, CVE-2023-22087, CVE-2023-27534, CVE-2023-22102, CVE-2020-11988, CVE-2019-17498, CVE-2023-22101, CVE-2023-22094, CVE-2023-22100, CVE-2023-2603, CVE-2023-26604, CVE-2023-29491, CVE-2023-35788, CVE-2020-36518, CVE-2020-7760, CVE-2021-28165, CVE-2021-37136, CVE-2021-37714, CVE-2021-40690, CVE-2021-43045, CVE-2022-23491, CVE-2022-24839, CVE-2022-25647, CVE-2022-29546, CVE-2022-3171, CVE-2022-40152, CVE-2022-41409, CVE-2022-41881, CVE-2022-41966, CVE-2022-42003, CVE-2022-42004, CVE-2022-43680, CVE-2022-4492, CVE-2022-45061, CVE-2022-45688, CVE-2022-45690, CVE-2022-4899, CVE-2023-0568, CVE-2023-1370, CVE-2023-1436, CVE-2023-20883, CVE-2023-22019, CVE-2023-22086, CVE-2023-22108, CVE-2023-24998, CVE-2023-28709, CVE-2023-30589, CVE-2023-30861, CVE-2023-34396, CVE-2023-34981, CVE-2023-3635, CVE-2023-38545, CVE-2023-0361, CVE-2019-10086, CVE-2022-48285, CVE-2023-22098, CVE-2023-22099, CVE-2022-33980, CVE-2023-2976, CVE-2023-30535, CVE-2021-37533, CVE-2022-40982, CVE-2023-20863, CVE-2023-22059, CVE-2023-22079, CVE-2023-22090, CVE-2023-22093, CVE-2023-22095, CVE-2023-22106, CVE-2023-22118, CVE-2023-2283, CVE-2023-23931, CVE-2023-2650, CVE-2023-28484, CVE-2023-38039, CVE-2023-20862, CVE-2023-22127, CVE-2020-11023, CVE-2022-29577, CVE-2022-36033, CVE-2023-22029, CVE-2023-22076, CVE-2023-22080, CVE-2023-22107, CVE-2023-28439, CVE-2023-41080, CVE-2022-44729, CVE-2023-22043, CVE-2023-22071, CVE-2023-22119, CVE-2023-22122, CVE-2023-22130, CVE-2021-36374, CVE-2023-22129, CVE-2021-41165, CVE-2023-22082, CVE-2023-22105, CVE-2023-22117, CVE-2023-22121, CVE-2023-22123, CVE-2023-22124, CVE-2023-22125, CVE-2020-13956, CVE-2022-24329, CVE-2022-37436, CVE-2023-22067, CVE-2023-22081, CVE-2023-22126, CVE-2023-26048, CVE-2023-26049, CVE-2023-33201, CVE-2023-34462, CVE-2023-3817, CVE-2023-40167, CVE-2023-22015, CVE-2023-22026, CVE-2023-22028, CVE-2023-22032, CVE-2023-22064, CVE-2023-22065, CVE-2023-22066, CVE-2023-22068, CVE-2023-22070, CVE-2023-22077, CVE-2023-22078, CVE-2023-22084, CVE-2023-22097, CVE-2023-22103, CVE-2023-22104, CVE-2023-22110, CVE-2023-22111, CVE-2023-22112, CVE-2023-22114, CVE-2023-22115, CVE-2023-22091, CVE-2023-

4039, CVE-2023-22109, CVE-2023-22073, CVE-2023-22083, CVE-2023-22088, CVE-2023-22096, CVE-2023-28708, CVE-2023-3247, CVE-2023-35887, CVE-2023-22025, CVE-2022-31160, CVE-2022-41954, CVE-2023-22128, CVE-2023-35116, CVE-2023-22113, CVE-2023-22074, CVE-2023-22075

- Oracle Critical Patch Update Advisory - October 2023
- VRM Vulnerability Reports