ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Mises à jour de sécurité pour plusieurs produits d'oracle
Numéro de Référence	42912007/23
Date de Publication	20 Juillet 2023
Risque	Important
Impact	Critique

Systèmes affectés

- Application Management Pack for Oracle Utilities & Enterprise Taxation, versions 13.4.1.0.0, 13.5.1.0.0
- BI Publisher, versions 6.4.0.0.0, 7.0.0.0.0
- JD Edwards EnterpriseOne Orchestrator, versions prior to 9.2.7.4
- JD Edwards EnterpriseOne Tools, versions prior to 9.2.7.4
- MySQL Cluster, versions 8.0.33 and prior
- MySQL Connectors, versions 8.0.33 and prior
- MySQL Enterprise Monitor, versions 8.0.34 and prior
- MySQL Server, versions 5.7.42 and prior, 8.0.33 and prior
- MySQL Workbench, versions 8.0.33 and prior
- Oracle Access Manager, version 12.2.1.4.0
- Oracle Agile Engineering Data Management, versions 6.2.1.0-6.2.1.8
- Oracle Agile PLM, version 9.3.6
- Oracle Application Express, versions [Application Express Administration] 18.2-22.2, [Application Express Customers Plugin] 18.2-22.2, [Application Express Team Calendar Plugin] 18.2-22.1
- Oracle Application Testing Suite, version 13.3.0.1
- Oracle AutoVue, versions 21.0.2.0-21.0.2.7
- Oracle Autovue for Agile Product Lifecycle Management, version 21.0.2
- Oracle BAM (Business Activity Monitoring), version 12.2.1.4.0
- Oracle Banking APIs, versions 18.2.0.0.0, 18.3.0.0.0, 19.1.0.0.0, 19.2.0.0.0, 21.1.0.0.0, 22.1.0.0.0, 22.2.0.0.0
- Oracle Banking Branch, versions 14.5-14.7
- Oracle Banking Cash Management, versions 14.7.0.2.0, 14.7.1.0.0

- Oracle Banking Corporate Lending, versions 14.0-14.3, 14.5-14.7
- Oracle Banking Corporate Lending Process Management, versions 14.4-14.7
- Oracle Banking Credit Facilities Process Management, version 14.7.1.0.0
- Oracle Banking Digital Experience, versions 18.2.0.0.0, 18.3.0.0.0, 19.1.0.0.0, 19.2.0.0.0, 21.1.0.0.0, 22.1.0.0.0, 22.2.0.0.0
- Oracle Banking Liquidity Management, versions 14.5.0.8.0, 14.6.0.3.0, 14.6.0.4.0, 14.7.0.1.0, 14.7.0.2.0, 14.7.1.0.0
- Oracle Banking Origination, versions 14.5-14.7, 14.7.0
- Oracle Banking Payments, versions 14.5-14.7
- Oracle Banking Supply Chain Finance, versions 14.7.0.2.0, 14.7.1.0.0
- Oracle Banking Trade Finance, versions 14.0-14.3, 14.5-14.7
- Oracle Banking Trade Finance Process Management, versions 14.5.0.8.0, 14.6.0.4.0, 14.7.0.2.0, 14.7.1.0.0
- Oracle Banking Treasury Management, versions 14.5-14.7
- Oracle Big Data Spatial and Graph, version 3.0
- Oracle Business Intelligence Enterprise Edition, versions 6.4.0.0.0, 7.0.0.0.0, 12.2.1.4.0
- Oracle Business Process Management Suite, version 12.2.1.4.0
- Oracle Coherence, versions 12.2.1.4.0, 14.1.1.0.0
- Oracle Commerce Guided Search, version 11.3.2
- Oracle Commerce Platform, versions 11.3.0, 11.3.1, 11.3.2
- Oracle Communications Billing and Revenue Management, versions 12.0.0.4.0-12.0.0.8.0
- Oracle Communications BRM - Elastic Charging Engine, versions 12.0.0.4.0-12.0.0.8.0
- Oracle Communications Calendar Server, versions 8.0.0.2.0-8.0.0.7.0
- Oracle Communications Cloud Native Core Automated Test Suite, versions 22.4.1, 23.1.0, 23.1.1
- Oracle Communications Cloud Native Core Binding Support Function, versions 22.4.0, 23.1.0
- Oracle Communications Cloud Native Core Console, versions 22.4.2, 23.1.1
- Oracle Communications Cloud Native Core Network Exposure Function, versions 22.4.3, 23.1.2
- Oracle Communications Cloud Native Core Network Function Cloud Native Environment, version 23.1.0
- Oracle Communications Cloud Native Core Network Repository Function, versions 22.4.2, 22.4.3, 23.1.0, 23.1.1, 23.2.0
- Oracle Communications Cloud Native Core Policy, versions 22.4.0, 23.1.0, 23.2.0
- Oracle Communications Cloud Native Core Security Edge Protection Proxy, versions 22.3.2, 22.4.0, 22.4.3, 23.1.0, 23.1.1, 23.1.2
- Oracle Communications Cloud Native Core Service Communication Proxy, versions 22.4.0, 23.1.0
- Oracle Communications Cloud Native Core Unified Data Repository, version 23.1.1
- Oracle Communications Contacts Server, versions 8.0.0.6.0-8.0.0.8.0
- Oracle Communications Converged Application Server - Service Controller, version 6.2.0
- Oracle Communications Convergence, version 3.0.3.2
- Oracle Communications Convergent Charging Controller, versions 12.0.3.0.0-12.0.6.0.0
- Oracle Communications Design Studio, versions 7.4.0.7.0, 7.4.1.5.0, 7.4.2.8.0

- Oracle Communications Diameter Signaling Router, version 8.6.0.0
- Oracle Communications Instant Messaging Server, version 10.0.1.7.0
- Oracle Communications Messaging Server, version 8.1.0.21.0
- Oracle Communications Network Analytics Data Director, version 23.1.0
- Oracle Communications Network Charging and Control, versions 12.0.3.0.0-12.0.6.0.0
- Oracle Communications Network Integrity, version 7.3.6.4
- Oracle Communications Operations Monitor, versions 5.0, 5.1
- Oracle Communications Order and Service Management, versions 7.3.5, 7.4.0, 7.4.1
- Oracle Communications Pricing Design Center, versions 12.0.0.4.0-12.0.0.7.0
- Oracle Communications Unified Assurance, versions 5.5.0-5.5.17, 6.0.0-6.0.2
- Oracle Communications Unified Inventory Management, versions 7.4.0-7.4.2, 7.5.0
- Oracle Data Integrator, version 12.2.1.4.0
- Oracle Database Server, versions 19.3-19.19, 21.3-21.10
- Oracle Documaker, versions 12.6.1-12.7.1
- Oracle E-Business Suite, versions 12.2.3-12.3.12
- Oracle Enterprise Data Quality, version 12.2.1.4.0
- Oracle Enterprise Manager for Exadata, version 13.5.0.0
- Oracle Enterprise Manager for Fusion Middleware, version 13.5.0.0
- Oracle Enterprise Manager for Oracle Database, version 13.5.0.0
- Oracle Enterprise Manager Ops Center, version 12.4.0.0
- Oracle Enterprise Operations Monitor, versions 5.0, 5.1
- Oracle Essbase, version 21.4.3.0.0
- Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.7, 8.0.8, 8.1.0, 8.1.1, 8.1.2
- Oracle Financial Services Behavior Detection Platform, versions 8.0.8.1, 8.1.1.1, 8.1.2.4, 8.1.2.5
- Oracle Financial Services Compliance Studio, version 8.1.2.4
- Oracle Financial Services Enterprise Case Management, versions 8.0.8.2, 8.1.1.1, 8.1.2.4, 8.1.2.5
- Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition, version 8.0.8
- Oracle FLEXCUBE Investor Servicing, version 14.7.0.0.0
- Oracle FLEXCUBE Universal Banking, versions 14.0-14.7
- Oracle Fusion Middleware MapViewer, version 12.2.1.4.0
- Oracle GoldenGate, versions 19.1.0.0.0-19.1.0.0.230422, 21.3.0.0.0-21.10.0.0.5
- Oracle GoldenGate Stream Analytics, versions 19.1.0.0.0-19.1.0.0.7
- Oracle GraalVM Enterprise Edition, versions 20.3.10, 21.3.6, 22.3.2
- Oracle GraalVM for JDK, versions 17.0.7, 20.0.1
- Oracle Graph Server and Client, versions 21.4.6, 21.4.7, 22.4.1, 22.4.2, 23.1.0
- Oracle Health Sciences Sciences Data Management Workbench, versions 3.1.0.2, 3.1.1.3, 3.2.0.0
- Oracle Hospitality Cruise Shipboard Property Management System, versions 20.1.0, 20.2.0, 20.3.3
- Oracle Hospitality Simphony, version 19.5
- Oracle HTTP Server, version 12.2.1.4.0

- Oracle Hyperion Data Relationship Management, version 11.2.13.0.0
- Oracle Hyperion Essbase Administration Services, version 21.4.3.0.0
- Oracle Hyperion Financial Reporting, version 11.2.13.0.0
- Oracle Hyperion Workspace, version 11.2.13.0.0
- Oracle Identity Manager, version 12.2.1.4.0
- Oracle Identity Manager Connector, versions 9.1.0, 12.2.1.3.0
- Oracle Java SE, versions 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1
- Oracle JDeveloper, version 12.2.1.4.0
- Oracle Middleware Common Libraries and Tools, version 12.2.1.4.0
- Oracle Mobile Security Suite, versions prior to 11.1.2.3.1
- Oracle NoSQL Database, versions 19.5.33, 20.3.28, 21.2.55, 22.3.26
- Oracle Policy Automation, versions prior to 12.2.31
- Oracle Retail Advanced Inventory Planning, versions 15.0, 16.0
- Oracle Retail Bulk Data Integration, versions 16.0.3, 19.0.1
- Oracle Retail Financial Integration, versions 14.2.0, 15.0.4, 16.0.3, 19.0.1
- Oracle Retail Integration Bus, versions 14.2.0, 15.0.4, 16.0.3, 19.0.1
- Oracle Retail Order Broker, version 19.1
- Oracle Retail Predictive Application Server, versions 15.0.3, 16.0.3
- Oracle Retail Service Backbone, versions 14.2.0, 15.0.4, 16.0.3, 19.0.1
- Oracle SD-WAN Edge, version 9.1.1.5.0
- Oracle Secure Backup, version 18.1.0.1.0
- Oracle Service Bus, version 12.2.1.4.0
- Oracle SOA Suite, version 12.2.1.4.0
- Oracle Solaris, version 11
- Oracle Spatial Studio, version 22.3.0
- Oracle TimesTen In-Memory Database, versions 22.1.1.1.0-22.1.1.11.0
- 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, 4.5.0.1.0, 4.5.0.1.1
- Oracle Utilities Network Management System, versions 2.4.0.1.21, 2.5.0.0.9, 2.5.0.1, 2.5.0.1.11, 2.5.0.2, 2.5.0.2.3, 2.6.0.0
- Oracle Utilities Testing Accelerator, versions 6.0.0.1-7.0.0.0
- Oracle VM VirtualBox, versions prior to 6.1.46, prior to 7.0.10
- Oracle WebCenter Content, version 12.2.1.4.0
- Oracle WebCenter Sites, version 12.2.1.4.0
- Oracle WebLogic Server, versions 12.2.1.4.0, 14.1.1.0.0
- PeopleSoft Enterprise PeopleTools, versions 8.59, 8.60
- Primavera Gateway, versions 18.8.0-18.8.15, 19.12.0-19.12.16, 20.12.0-20.12.11, 21.12.0-21.12.9
- Primavera P6 Enterprise Project Portfolio Management, versions 22.12.2, 22.12.3
- Primavera Unifier, versions 18.8.0-18.8.18, 19.12.0-19.12.16, 20.12.0-20.12.16, 21.12.0-21.12.15, 22.12.0-22.12.6
- Siebel Applications, versions 22.12 and prior, 23.6 and prior

Identificateurs externes

Les CVE identifiants les vulnérabilités peuvent être consultés sur le bulletin d'Oracle :

- https://www.oracle.com/security-alerts/cpujul2023.html

Bilan de la vulnérabilité

Oracle a publié des correctifs de sécurité pour corriger plusieurs vulnérabilités dans le cadre de sa mise à jour trimestrielle. Les vulnérabilités traitées par ces correctifs touchent des dizaines de produits cités au niveau de ce bulletin.
Un attaquant distant non authentifié peut exploiter ces vulnérabilités pour exécuter du code arbitraire, accéder à des données confidentielles ou causer un déni de service.

Solution

Veuillez se référer au bulletin de sécurité d'Oracle afin d'installer les nouvelles mises à jour.

Risque

- Exécution de code arbitraire à distance.
- Accès à des informations confidentielles.
- Déni de service.

Référence

Bulletins de sécurité d'Oracle :

- https://www.oracle.com/security-alerts/cpujul2023.html