ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	"Oracle Critical Patch Update" du Mois Juillet 2022
Numéro de Référence	37342007/22
Date de Publication	20 juillet 2022
Risque	Critique
Impact	Critique

Systèmes affectés

- Autonomous Health Framework
- Big Data Spatial and Graph, versions version antérieure à 23.1
- Enterprise Manager Base Platform, versions 13.4.0.0, 13.5.0.0
- Enterprise Manager for MySQL Database
- Enterprise Manager Ops Center, version 12.4.0.0
- JD Edwards EnterpriseOne Orchestrator, versions 9.2.6.3 et version antérieure
- JD Edwards EnterpriseOne Tools, versions 9.2.6.3 et version antérieure
- MySQL Cluster, versions 7.4.36 et version antérieure, 7.5.26 et version antérieure, 7.6.22 et version antérieure, 8.0.29 et version antérieure, and8.0.29 et version antérieure
- MySQL Enterprise Monitor, versions 8.0.30 et version antérieure
- MySQL Server, versions 5.7.38 et version antérieure, 8.0.29 et version antérieure
- MySQL Shell, versions 8.0.28 et version antérieure
- MySQL Shell for VS Code, versions 1.1.8 et version antérieure
- MySQL Workbench, versions 8.0.29 et version antérieure
- Oracle Agile Engineering Data Management, version 6.2.1.0
- Oracle Agile PLM, version 9.3.6
- Oracle Agile Product Lifecycle Management for Process, versions 6.2.2, 6.2.3
- Oracle Application Express, versions version antérieure à 22.1.1
- Oracle Application Testing Suite, version 13.3.0.1
- Oracle Autovue for Agile Product Lifecycle Management, version 21.0.2
- Oracle Banking Branch, version 14.5

- Oracle Banking Cash Management, version 14.5
- Oracle Banking Corporate Lending Process Management, version 14.5
- Oracle Banking Credit Facilities Process Management, version 14.5
- Oracle Banking Deposits and Lines of Credit Servicing, version 2.7
- Oracle Banking Electronic Data Exchange for Corporates, version 14.5
- Oracle Banking Liquidity Management, versions 14.2, 14.5
- Oracle Banking Origination, version 14.5
- Oracle Banking Party Management, version 2.7
- Oracle Banking Platform, versions 2.6.2, 2.9, 2.12
- Oracle Banking Supply Chain Finance, version 14.5
- Oracle Banking Trade Finance, version 14.5
- Oracle Banking Trade Finance Process Management, version 14.5
- Oracle Banking Virtual Account Management, version 14.5
- Oracle Berkeley DB
- Oracle BI Publisher, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle Blockchain Platform
- Oracle Business Intelligence Enterprise Edition, version 5.9.0.0.0
- Oracle Coherence, versions 3.7.1.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0
- Oracle Commerce Guided Search, version 11.3.2
- Oracle Commerce Merchandising, version 11.3.2
- Oracle Commerce Platform, versions 11.3.0, 11.3.1, 11.3.2
- Oracle Communications ASAP, version 7.3
- Oracle Communications Billing and Revenue Management, versions 12.0.0.4.0-12.0.0.6.0
- Oracle Communications BRM - Elastic Charging Engine, versions version antérieure à 12.0.0.4.6, version antérieure à 12.0.0.5.1
- Oracle Communications Cloud Native Core Binding Support Function, versions 22.1.3, 22.2.0
- Oracle Communications Cloud Native Core Console, versions 22.1.2, 22.2.0
- Oracle Communications Cloud Native Core Network Exposure Function, version 22.1.1
- Oracle Communications Cloud Native Core Network Function Cloud Native Environment, versions 22.1.0, 22.1.2, 22.2.0
- Oracle Communications Cloud Native Core Network Repository Function, versions 22.1.2, 22.2.0

- Oracle Communications Cloud Native Core Network Slice Selection Function, version 22.1.1
- Oracle Communications Cloud Native Core Policy, versions 22.1.3, 22.2.0
- Oracle Communications Cloud Native Core Security Edge Protection Proxy, version 22.1.1
- Oracle Communications Cloud Native Core Service Communication Proxy, version 22.2.0
- Oracle Communications Cloud Native Core Unified Data Repository, version 22.2.0
- Oracle Communications Core Session Manager, versions 8.2.5, 8.4.5
- Oracle Communications Design Studio, version 7.4.2
- Oracle Communications Instant Messaging Server, version 10.0.1.5.0
- Oracle Communications IP Service Activator
- Oracle Communications Offline Mediation Controller, versions version antérieure à 12.0.0.4.4, version antérieure à 12.0.0.5.1
- Oracle Communications Operations Monitor, versions 4.3, 4.4, 5.0
- Oracle Communications Session Border Controller, versions 8.4, 9.0, 9.1
- Oracle Communications Unified Inventory Management, versions 7.4.1, 7.4.2, 7.5.0
- Oracle Communications Unified Session Manager, version 8.2.5
- Oracle Crystal Ball, versions 11.1.2.0.0-11.1.2.4.900
- Oracle Data Integrator
- Oracle Database Server, versions 12.1.0.2, 19c, 21c
- Oracle E-Business Suite, versions 12.2.3-12.2.11
- Oracle Enterprise Communications Broker, version 3.3
- Oracle Enterprise Operations Monitor, versions 4.3, 4.4, 5.0
- Oracle Enterprise Session Border Controller, versions 8.4, 9.0, 9.1
- Oracle Essbase, version 21.3
- Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.7.0-8.1.0.0, 8.1.1.0, 8.1.2.0, 8.1.2.1
- Oracle Financial Services Behavior Detection Platform, versions 8.0.7.0, 8.0.8.0, 8.1.1.0-8.1.2.1
- Oracle Financial Services Crime and Compliance Management Studio, versions 8.0.8.2.0, 8.0.8.3.0
- Oracle Financial Services Enterprise Case Management, versions 8.0.7.1, 8.0.7.2, 8.0.8.0, 8.0.8.1, 8.1.1.0-8.1.2.1
- Oracle Financial Services Revenue Management and Billing, versions 2.9.0.0.0, 2.9.0.1.0, 3.0.0.0.0-3.2.0.0.0, 4.0.0.0.0

- Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition, versions 8.0.7.0, 8.0.8.0
- Oracle FLEXCUBE Core Banking, versions 5.2, 11.6-11.8, 11.10
- Oracle FLEXCUBE Private Banking, version 12.1
- Oracle FLEXCUBE Universal Banking, versions 12.1-12.4, 14.0-14.3, 14.5
- Oracle Global Lifecycle Management NextGen OUI Framework, versions version antérieure à 13.9.4.2.10
- Oracle Global Lifecycle Management OPatch, versions version antérieure à 12.2.0.1.30
- Oracle GoldenGate, versions [19c] version antérieure à 19.1.0.0.220719, [21c] version antérieure à 21.7.0.0.0
- Oracle GraalVM Enterprise Edition, versions 20.3.6, 21.3.2, 22.1.0
- Oracle Graph Server and Client, versions version antérieure à 22.2.0
- Oracle Health Sciences Data Management Workbench, versions 2.4.8.7, 2.5.2.1, 3.0.0.0, 3.1.0.3
- Oracle Health Sciences Empirica Signal, versions 9.1.0.52, 9.2.0.52
- Oracle Health Sciences Information Manager, versions 3.0.0.1, 3.0.1.0-3.0.5.0
- Oracle Healthcare Foundation, versions 8.1.0, 8.2.0, 8.2.1
- Oracle Hospitality Cruise Shipboard Property Management System, version 20.2.1
- Oracle Hospitality Inventory Management, version 9.1
- Oracle Hospitality Materials Control, version 18.1
- Oracle Hospitality OPERA 5, version 5.6
- Oracle HTTP Server, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle Identity Management Suite
- Oracle Identity Manager Connector
- Oracle Java SE, versions 7u343, 8u333, 11.0.15.1, 17.0.3.1, 18.0.1.1
- Oracle Managed File Transfer, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle Middleware Common Libraries and Tools, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle NoSQL Database
- Oracle Policy Automation, versions 12.2.0-12.2.25
- Oracle Policy Automation for Mobile Devices, versions 12.2.0-12.2.24
- Oracle Product Lifecycle Analytics, version 3.6.1
- Oracle REST Data Services, versions version antérieure à 22.1.1
- Oracle Retail Allocation, versions 15.0.3.1, 16.0.3
- 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, 18.0, 19.0
- Oracle Retail Extract Transform and Load, version 13.2.5
- Oracle Retail Financial Integration, versions 14.1.3.2, 15.0.3.1, 16.0.3, 19.0.1
- Oracle Retail Integration Bus, versions 14.1.3.2, 15.0.3.1, 16.0.3, 19.0.1
- Oracle Retail Merchandising System, versions 16.0.3, 19.0.1
- Oracle Retail Order Broker, versions 18.0, 19.1
- Oracle Retail Pricing, version 19.0.1
- Oracle Retail Sales Audit, versions 15.0.3.1, 16.0.3
- Oracle Retail Xstore Point of Service, versions 17.0.4, 18.0.3, 19.0.2, 20.0.1, 21.0.1
- Oracle SD-WAN Edge, versions 9.0, 9.1
- Oracle Security Service, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle SOA Suite, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle Solaris, versions 10, 11
- Oracle Spatial Studio, versions version antérieure à 22.1.0
- Oracle SQL Developer
- Oracle Stream Analytics, versions [19c] version antérieure à 19.1.0.0.6.4
- Oracle TimesTen In-Memory Database, versions version antérieure à 22.1.1.1.0
- Oracle Transportation Management, version 1.4.4
- Oracle Utilities Framework, versions 4.3.0.5.0, 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
- Oracle VM VirtualBox, versions version antérieure à 6.1.36
- Oracle WebCenter Content, 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 Support Tools, versions version antérieure à 4.4.2
- Oracle WebLogic Server, versions 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0
- Oracle Weblogic Server Proxy Plug-in, versions 12.2.1.3.0, 12.2.1.4.0
- Oracle ZFS Storage Appliance Kit, version 8.8
- PeopleSoft Enterprise PeopleTools, versions 8.58, 8.59
- Primavera Gateway, versions 17.12.0-17.12.11, 18.8.0-18.8.14, 19.12.0-19.12.13, 20.12.0-20.12.8, 21.12.0-21.12.1
- Primavera P6 Enterprise Project Portfolio Management, versions 17.12.0.0-17.12.20.4, 18.8.0.0-18.8.25.4, 19.12.0.0-19.12.19.0, 20.12.0.0-20.12.14.0, 21.12.0.0-21.12.4.0

- Primavera Unifier, versions 17.7-17.12, 18.8, 19.12, 20.12, 21.12
- Siebel Applications, versions 22.6 et version antérieure

Identificateurs externes

- CVE-2022-22965 CVE-2020-10683 CVE-2022-22947 CVE-2022-22963 CVE-2022-1292 CVE-2021-31805 CVE-2021-23926 CVE-2021-29921 CVE-2019-17571 CVE-2019-9636 CVE-2018-1273 CVE-2022-22978 CVE-2021-3177 CVE-2022-23305 CVE-2022-23307 CVE-2022-23302 CVE-2020-1747 CVE-2019-10082 CVE-2021-29505 CVE-2022-23218 CVE-2021-3773 CVE-2022-22720 CVE-2021-22931 CVE-2021-2351 CVE-2021-26291 CVE-2022-25845 CVE-2022-22721 CVE-2021-39146 CVE-2022-23806 CVE-2022-23219 CVE-2022-1154 CVE-2020-14343 CVE-2022-24407 CVE-2020-27619 CVE-2021-41303 CVE-2021-39144 CVE-2021-39150 CVE-2021-39152 CVE-2021-39153 CVE-2019-0219 CVE-2022-25762 CVE-2022-21543 CVE-2022-21510 CVE-2020-35169 CVE-2022-0839 CVE-2020-29506 CVE-2020-29507 CVE-2020-29508 CVE-2020-35163 CVE-2020-35166 CVE-2020-35167 CVE-2020-35168 CVE-2020-29396 CVE-2019-17495 CVE-2022-23632 CVE-2020-9492 CVE-2021-42575 CVE-2022-23457 CVE-2021-23450 CVE-2021-39139 CVE-2021-39141 CVE-2021-39145 CVE-2021-39147 CVE-2021-39148 CVE-2021-39149 CVE-2021-39151 CVE-2021-39154

Bilan de la vulnérabilité

Oracle a publié des correctifs de sécurité pour traiter plusieurs vulnérabilités dans le cadre de sa mise à jour « Oracle Critical Patch Update » du mois Juillet 2022. L'exploitation de certaines de ces vulnérabilités pourrait permettre à un attaquant distant de prendre le contrôle d'un système affecté, d'exécuter du code arbitraire à distance, de contourner la politique de sécurité, de causer un déni de service à distance ou de porter atteinte à la confidentialité de données.

Solution

Veuillez se référer au bulletin de sécurité Oracle du 19 Juillet 2022, afin d'installer les dernières mises à jour de sécurité.

Risque

- Déni de service à distance,
- Exécution du code arbitraire à distance,
- Contournement de la politique de sécurité,
- Atteinte à la confidentialité,
- Prise contrôle du système,

Annexe

Bulletin de sécurité Oracle du 19 Juillet 2022**:**

- https://www.oracle.com/security-alerts/cpujul2022.html