



BULLETIN DE SECURITE

Titre	"Oracle Critical Patch Update" du Mois Avril 2023
Numéro de Référence	41421904/23
Date de Publication	19 Avril 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- JD Edwards EnterpriseOne Orchestrator, versions antérieures à 9.2.7.3
- JD Edwards EnterpriseOne Tools, versions antérieures à 9.2.7.3
- JD Edwards World Security, version A9.4
- Management Cloud Engine, version 22.1.0.0.0
- MySQL Cluster, versions 7.5.29 et antérieures, 7.6.25 et antérieures, 8.0.32 et antérieures
- MySQL Connectors, versions 8.0.32 et antérieures
- MySQL Enterprise Monitor, versions 8.0.33 et antérieures
- MySQL Server, versions 5.7.41 et antérieures, 8.0.32 et antérieures
- MySQL Workbench, versions 8.0.32 et antérieures
- Oracle Access Manager, version 12.2.1.4.0
- Oracle Agile PLM, version 9.3.6
- Oracle Application Testing Suite, version 13.3.0.1
- Oracle Argus Insight, versions antérieures à 8.2.3
- Oracle Argus Safety, versions antérieures à 8.2.3
- Oracle BI Publisher, versions 6.4.0.0.0, 12.2.1.4.0
- Oracle Banking APIs, versions 18.2, 18.3, 19.1, 19.2, 21.1, 22.1, 22.2
- Oracle Banking Corporate Lending Process Management, versions 14.4-14.7
- Oracle Banking Corporate Lending, versions 14.0-14.3, 14.5-14.7
- Oracle Banking Digital Experience, versions 18.2, 18.3, 19.1, 19.2, 21.1, 22.1, 22.2
- Oracle Banking Payments, versions 14.5, 14.6, 14.7

- Oracle Banking Trade Finance, versions 14.5, 14.6, 14.7
- Oracle Banking Treasury Management, versions 14.5, 14.6, 14.7
- Oracle Banking Virtual Account Management, versions 14.5, 14.6, 14.7
- Oracle Big Data Spatial and Graph, versions antérieures à 23.1
- Oracle Blockchain Platform, versions antérieures à 21.1.3
- Oracle Business Intelligence Enterprise Edition, versions 5.9.0.0.0, 6.4.0.0.0, 12.2.1.4.0
- Oracle Business Process Management Suite, version 12.2.1.4.0
- Oracle Clinical Remote Data Capture, version 5.4.0.2
- 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 Cloud Native Configuration Console, versions 22.4.1, 23.1.0
- Oracle Communications Cloud Native Core Automated Test Suite, versions 22.3.1, 22.4.0
- Oracle Communications Cloud Native Core Binding Support Function, versions 22.4.0-22.4.4, 23.1.0-23.1.1
- Oracle Communications Cloud Native Core Console, versions 22.3.0, 22.4.0
- Oracle Communications Cloud Native Core Network Exposure Function, versions 22.4.2, 23.1.0
- Oracle Communications Cloud Native Core Network Function Cloud Native Environment, version 22.4.0
- Oracle Communications Cloud Native Core Network Repository Function, version 23.1.0
- Oracle Communications Cloud Native Core Policy, versions 22.4.0-22.4.4, 23.1.0-23.1.1
- Oracle Communications Cloud Native Core Security Edge Protection Proxy, versions 22.4.0, 22.4.1, 22.4.2, 23.1.0
- Oracle Communications Cloud Native Core Service Communication Proxy, versions 22.3.0, 22.4.0
- Oracle Communications Cloud Native Core Unified Data Repository, versions 22.4.1, 23.1.0
- Oracle Communications Convergent Charging Controller, versions 6.0.1.0.0, 12.0.1.0.0-12.0.6.0.0
- Oracle Communications Core Session Manager, versions 8.45, 9.15
- Oracle Communications Diameter Signaling Router, version 8.6.0.0
- Oracle Communications Element Manager, versions 9.0.0, 9.0.1
- Oracle Communications IP Service Activator, versions 7.4.0, 7.5.0

- Oracle Communications Network Charging and Control, versions 6.0.1.0.0, 12.0.1.0.0-12.0.6.0.0
- Oracle Communications Operations Monitor, version 5.0
- Oracle Communications Order and Service Management, version 7.4.1
- Oracle Communications Policy Management, version 12.6.0.0.0
- Oracle Communications Services Gatekeeper, version 7.0.0.0.0
- Oracle Communications Session Border Controller, versions 9.0, 9.1
- Oracle Communications Session Report Manager, versions 9.0.0, 9.0.1
- Oracle Communications Session Router, versions 9.0, 9.1
- Oracle Communications Subscriber-Aware Load Balancer, versions 9.0, 9.1
- Oracle Communications Unified Assurance, versions 5.5.0-5.5.10, 6.0.0-6.0.2
- Oracle Communications Unified Inventory Management, versions 7.4.0, 7.4.1, 7.4.2, 7.5.0
- Oracle Communications User Data Repository, version 12.6.1.0.0
- Oracle Data Integrator, version 12.2.1.4.0
- Oracle Database Server, versions 19c, 21c
- Oracle Documaker, versions 12.6.0.0.0, 12.6.2.0.0-12.6.4.0.0, 12.7.0.0.0, 12.7.1.0.0
- Oracle E-Business Suite, versions 12.2.3-12.2.12
- Oracle Enterprise Communications Broker, versions 3.3, 4.0
- Oracle Enterprise Manager Ops Center, version 12.4.0.0
- Oracle Enterprise Session Router, version 9.1
- Oracle Essbase, version 21.4
- Oracle FLEXCUBE Core Banking, versions 11.6, 11.7, 11.8, 11.10, 11.11
- Oracle FLEXCUBE Universal Banking, versions 14.0-14.3, 14.5-14.7
- Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.7.0, 8.0.8.0, 8.0.9.0, 8.1.0.0, 8.1.1.0, 8.1.2.0, 8.1.2.1, 8.1.2.2
- Oracle Financial Services Analytical Applications Reconciliation Framework, versions 8.0.7.1.2, 8.1.1.1.7
- Oracle Financial Services Asset Liability Management, version 8.0.7.8.0
- Oracle Financial Services Balance Computation Engine, version 8.1.1.1.1
- Oracle Financial Services Balance Sheet Planning, version 8.0.8.1.4
- Oracle Financial Services Behavior Detection Platform, versions 8.0.8.1, 8.1.1.1, 8.1.2.3, 8.1.2.4
- Oracle Financial Services Compliance Studio, version 8.1.2.4
- Oracle Financial Services Crime and Compliance Management Studio, version 8.0.8.3.5

- Oracle Financial Services Currency Transaction Reporting, versions 8.0.8.1.0, 8.1.1.1.0, 8.1.2.3.0, 8.1.2.4.1
- Oracle Financial Services Data Governance for US Regulatory Reporting, versions 8.1.2.0, 8.1.2.1
- Oracle Financial Services Data Integration Hub, versions 8.0.7.3.1, 8.1.0.1.4, 8.1.2.2.1
- Oracle Financial Services Deposit Insurance Calculations for Liquidity Risk Management, versions 8.0.7.3.1, 8.0.8.3.1
- Oracle Financial Services Enterprise Case Management, versions 8.0.8.2, 8.1.1.1, 8.1.2.3, 8.1.2.4
- Oracle Financial Services Enterprise Financial Performance Analytics, version 8.0.7.8.1
- Oracle Financial Services Funds Transfer Pricing, version 8.0.7.8.1
- Oracle Financial Services Institutional Performance Analytics, version 8.0.7.8.1
- Oracle Financial Services Liquidity Risk Measurement and Management, versions 8.0.7.3.1, 8.0.8.3.1
- Oracle Financial Services Loan Loss Forecasting and Provisioning, versions 8.0.7.8.1, 8.0.8.2.1
- Oracle Financial Services Model Management and Governance, versions 8.1.0.0, 8.1.2.0
- Oracle Financial Services Profitability Management, version 8.0.7.8.1
- Oracle Financial Services Regulatory Reporting with AgileREPORTER, version 8.1.1.2.0
- Oracle Financial Services Regulatory Reporting, versions 8.0.8.1, 8.1.1.1, 8.1.2.3, 8.1.2.4
- Oracle Financial Services Retail Performance Analytics, version 8.0.7.8.1
- Oracle Financial Services Revenue Management and Billing, versions 2.7, 2.7.1, 2.8, 2.9, 2.9.1, 3.0, 3.1, 3.2, 4.0
- Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition, version 8.0.8.0.0
- Oracle GoldenGate Studio, version [Fusion Middleware] 12.2.1.4.0
- Oracle GoldenGate, versions antérieures à 19.1.0.0.230418, antérieures à 21.10.0.0.0
- Oracle GraalVM Enterprise Edition, versions 20.3.8, 20.3.9, 21.3.4, 21.3.5, 22.3.0, 22.3.1
- Oracle Graph Server and Client, versions antérieures à 23.1.0, antérieures à 23.2.0
- Oracle HTTP Server, version 12.2.1.4.0
- Oracle Health Sciences InForm, versions antérieures à 6.3.1.3, antérieures à 7.0.0.1
- Oracle Healthcare Foundation, versions 8.1.0, 8.1.1, 8.2.0, 8.2.1, 8.2.2
- Oracle Healthcare Master Person Index, versions 5.0.0-5.0.4
- Oracle Healthcare Translational Research, versions 4.1.0, 4.1.1

- Oracle Hospitality OPERA 5 Property Services, version 5.6
- Oracle Hyperion Financial Reporting, version 11.2.12
- Oracle Hyperion Infrastructure Technology, version 11.2.12
- Oracle Identity Manager, version 12.2.1.4.0
- Oracle Insurance Policy Administration Operational Data Store for Life and Annuity, version 1.0.1.8
- Oracle JDeveloper, version 12.2.1.4.0
- Oracle Java SE, versions 8u361, 8u361-perf, 11.0.18, 17.0.6, 20
- Oracle Managed File Transfer, version 12.2.1.4.0
- Oracle Middleware Common Libraries and Tools, version 12.2.1.4.0
- Oracle NoSQL Database, versions antérieures à 19.5.32
- Oracle Outside In Technology, version 8.5.6
- Oracle REST Data Services, versions antérieures à 23.1.0
- Oracle Retail Customer Management and Segmentation Foundation, versions 18.0.0.12, 19.0.0.6
- Oracle Retail Fiscal Management, version 14.2
- Oracle Retail Invoice Matching, versions 15.0.3, 16.0.3
- Oracle Retail Merchandising System, versions 15.0.3.1, 16.0.2, 16.0.3
- Oracle Retail Predictive Application Server, versions 15.0.3, 16.0.3
- Oracle Retail Price Management, versions 14.1.3.2, 15.0.3.1, 16.0.3
- Oracle Retail Sales Audit, version 15.0.3.1
- Oracle Retail Xstore Office Cloud Service, versions 18.0.5, 19.0.4, 20.0.3, 21.0.2
- Oracle Retail Xstore Point of Service, versions 17.0.6, 18.0.5, 19.0.4, 20.0.3, 21.0.2
- Oracle SD-WAN Aware, version 9.0.1.6.0
- Oracle SD-WAN Edge, versions 9.1.1.3.0, 9.1.1.4.0
- Oracle SOA Suite, version 12.2.1.4.0
- Oracle SQL Developer, versions antérieures à 22.4.0, antérieures à 23.1.0
- Oracle Solaris, versions 10, 11
- Oracle TimesTen In-Memory Database, versions antérieures à 22.1.1.7.0
- 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
- Oracle Utilities Network Management System, versions 2.3.0.2, 2.4.0.1, 2.5.0.0, 2.5.0.1, 2.5.0.2
- Oracle VM VirtualBox, versions antérieures à 6.1.44, antérieures à 7.0.8

- Oracle WebCenter Portal, version 12.2.1.4.0
- Oracle WebCenter Sites, version 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 iLearning, version 6.3.1
- PeopleSoft Enterprise HCM Human Resources, version 9.2
- PeopleSoft Enterprise PeopleTools, versions 8.58, 8.59, 8.60
- Primavera P6 Enterprise Project Portfolio Management, versions 18.8.0-18.8.26, 19.12.0-19.12.21, 20.12.0-20.12.18, 21.12.0-21.12.12, 22.12.0-22.12.3
- Primavera Unifier, versions 18.8.0-18.8.18, 19.12.0-19.12.16, 20.12.0-20.12.16, 21.12.0-21.12.14, 22.12.0-22.12.3
- Siebel Applications, versions 21.10 et antérieures, 22.10 et antérieures, 23.3 et antérieures

Identificateurs externes

- CVE-2018-1311 , CVE-2018-14371 , CVE-2019-10086 , CVE-2019-10172 , CVE-2019-11287 , CVE-2019-12415 , CVE-2019-18935 , CVE-2019-20916 , CVE-2020-11987 , CVE-2020-11988 , CVE-2020-13936 , CVE-2020-13954 , CVE-2020-14343 , CVE-2020-15250 , CVE-2020-17521 , CVE-2020-25638 , CVE-2020-25649 , CVE-2020-28052 , CVE-2020-35168 , CVE-2020-35169 , CVE-2020-36518 , CVE-2020-6950 , CVE-2020-7009 , CVE-2020-7712 , CVE-2020-8908 , CVE-2021-22569 , CVE-2021-23017 , CVE-2021-23337 , CVE-2021-23413 , CVE-2021-2351 , CVE-2021-23926 , CVE-2021-27568 , CVE-2021-28168 , CVE-2021-29425 , CVE-2021-29921 , CVE-2021-30129 , CVE-2021-31684 , CVE-2021-34798 , CVE-2021-35043 , CVE-2021-36090 , CVE-2021-36373 , CVE-2021-36374 , CVE-2021-3712 , CVE-2021-37519 , CVE-2021-37533 , CVE-2021-37695 , CVE-2021-3918 , CVE-2021-4048 , CVE-2021-40528 , CVE-2021-40690 , CVE-2021-41183 , CVE-2021-41184 , CVE-2021-41973 , CVE-2021-42575 , CVE-2021-43859 , CVE-2021-44832 , CVE-2021-46848 , CVE-2022-1292 , CVE-2022-1471 , CVE-2022-1587 , CVE-2022-2048 , CVE-2022-21824 , CVE-2022-2274 , CVE-2022-22965 , CVE-2022-22971 , CVE-2022-22978 , CVE-2022-22979 , CVE-2022-23181 , CVE-2022-23219 , CVE-2022-23221 , CVE-2022-23305 , CVE-2022-23437 , CVE-2022-23457 , CVE-2022-23491 , CVE-2022-24729 , CVE-2022-24839 , CVE-2022-25315 , CVE-2022-25647 , CVE-2022-25857 , CVE-2022-26336 , CVE-2022-27404 , CVE-2022-27782 , CVE-2022-28199 , CVE-2022-28327 , CVE-2022-28738 , CVE-2022-29078 , CVE-2022-29577 , CVE-2022-29599 , CVE-2022-31081 , CVE-2022-31123 , CVE-2022-31129 , CVE-2022-31160 , CVE-2022-31630 , CVE-2022-31692 , CVE-2022-3171 , CVE-2022-32215 , CVE-2022-33980 , CVE-2022-34169 , CVE-2022-34305 , CVE-2022-3479 , CVE-2022-34917 , CVE-2022-35737 , CVE-2022-36033 , CVE-2022-36760 , CVE-2022-37434 , CVE-2022-37865 , CVE-2022-38752 , CVE-2022-39135 , CVE-2022-39271 , CVE-2022-40146 , CVE-2022-40149 , CVE-2022-40151 , CVE-2022-40152 , CVE-2022-40304 , CVE-2022-41715 , CVE-2022-41881 , CVE-2022-41966 , CVE-2022-42003 , CVE-2022-42004 , CVE-2022-42252 , CVE-2022-42889 , CVE-2022-42890 , CVE-2022-42898 , CVE-2022-42916 , CVE-2022-43401 , CVE-2022-43402 , CVE-2022-43548 , CVE-2022-43551 , CVE-2022-43680 , CVE-2022-4415 , CVE-2022-

45047 , CVE-2022-45061 , CVE-2022-45143 , CVE-2022-45685 , CVE-2022-45693 , CVE-2022-46364 , CVE-2022-46908 , CVE-2022-47629 , CVE-2023-0215 , CVE-2023-0361 , CVE-2023-0662 , CVE-2023-1370 , CVE-2023-21896 , CVE-2023-21902 , CVE-2023-21903 , CVE-2023-21904 , CVE-2023-21905 , CVE-2023-21906 , CVE-2023-21907 , CVE-2023-21908 , CVE-2023-21909 , CVE-2023-21910 , CVE-2023-21911 , CVE-2023-21912 , CVE-2023-21913 , CVE-2023-21915 , CVE-2023-21916 , CVE-2023-21917 , CVE-2023-21918 , CVE-2023-21919 , CVE-2023-21920 , CVE-2023-21921 , CVE-2023-21922 , CVE-2023-21923 , CVE-2023-21924 , CVE-2023-21925 , CVE-2023-21926 , CVE-2023-21927 , CVE-2023-21928 , CVE-2023-21929 , CVE-2023-21930 , CVE-2023-21931 , CVE-2023-21932 , CVE-2023-21933 , CVE-2023-21934 , CVE-2023-21935 , CVE-2023-21936 , CVE-2023-21937 , CVE-2023-21938 , CVE-2023-21939 , CVE-2023-21940 , CVE-2023-21941 , CVE-2023-21942 , CVE-2023-21943 , CVE-2023-21944 , CVE-2023-21945 , CVE-2023-21946 , CVE-2023-21947 , CVE-2023-21948 , CVE-2023-21952 , CVE-2023-21953 , CVE-2023-21954 , CVE-2023-21955 , CVE-2023-21956 , CVE-2023-21959 , CVE-2023-21960 , CVE-2023-21962 , CVE-2023-21963 , CVE-2023-21964 , CVE-2023-21965 , CVE-2023-21966 , CVE-2023-21967 , CVE-2023-21968 , CVE-2023-21969 , CVE-2023-21970 , CVE-2023-21971 , CVE-2023-21972 , CVE-2023-21973 , CVE-2023-21976 , CVE-2023-21977 , CVE-2023-21978 , CVE-2023-21979 , CVE-2023-21980 , CVE-2023-21981 , CVE-2023-21982 , CVE-2023-21984 , CVE-2023-21985 , CVE-2023-21986 , CVE-2023-21987 , CVE-2023-21988 , CVE-2023-21989 , CVE-2023-21990 , CVE-2023-21991 , CVE-2023-21992 , CVE-2023-21993 , CVE-2023-21996 , CVE-2023-21997 , CVE-2023-21998 , CVE-2023-21999 , CVE-2023-22000 , CVE-2023-22001 , CVE-2023-22002 , CVE-2023-22003 , CVE-2023-22899 , CVE-2023-23914 , CVE-2023-23916 , CVE-2023-23918 , CVE-2023-23931 , CVE-2023-24998 , CVE-2023-25136 , CVE-2023-25194 , CVE-2023-25577 , CVE-2023-25613 , CVE-2023-25690 , CVE-2023-28708

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 Avril 2023. 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 18 Avril 2023, 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 18 Avril 2023:

- <https://www.oracle.com/security-alerts/cpuapr2023verbose.html>
- <https://www.oracle.com/security-alerts/cpuapr2023.html>