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 Avril 2024
Numéro de Référence	47051804/24
Date de Publication	18 Avril 2024
Risque	Critique
Impact	Critique

Systèmes affectés

- Autonomous Health Framework, versionsantérieure à 23.11.1,antérieure à 24.2
- Management Cloud Engine, version 24.1.0.0.0
- MySQL Cluster, versions 7.5.33 et antérieure, 7.6.29 et antérieure, 8.0.36 et antérieure, 8.2.0 et antérieure, 8.3.0 et antérieure
- MySQL Connectors, versions 8.3.0 et antérieure
- MySQL Enterprise Backup, versions 8.0.36 et antérieure, 8.3.0 et antérieure
- MySQL Enterprise Monitor, versions 8.0.37 et antérieure
- MySQL Server, versions 8.0.36 et antérieure, 8.2.0 et antérieure, 8.3.0 et antérieure
- OPatch, versionsantérieure à 12.2.0.1.42
- OPatchAuto, versionsantérieure à 12.2.0.1.42
- Oracle Access Manager, version 12.2.1.4.0
- Oracle Agile PLM, version 9.3.6
- Oracle Agile Product Lifecycle Management for Process, version 6.2.4.2
- Oracle Application Testing Suite, version 13.3.0.1
- Oracle Banking APIs, versions 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 14.5.0.0.0, 14.6.0.0.0, 14.7.0.0.0
- Oracle Banking Cash Management, versions 14.5.0.0.0, 14.6.0.0.0, 14.7.0.0.0
- Oracle Banking Deposits et Lines of Credit Servicing, version 2.12.0.0.0
- Oracle Banking Digital Experience, versions 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 Enterprise Default Management, versions 2.7.0.0.0, 2.12.0.0.0

- Oracle Banking Liquidity Management, versions 14.5.0.0.0, 14.6.0.0.0, 14.7.0.0.0, 14.7.0.3.0
- Oracle Banking Loans Servicing, version 2.12.0.0.0
- Oracle Banking Origination, versions 14.5.0.0.0, 14.6.0.0.0, 14.7.0.0.0
- Oracle Banking Party Management, version 2.7.0.0.0
- Oracle Banking Platform, versions 2.7.0.0.0, 2.12.0.0.0
- Oracle Banking Virtual Account Management, versions 14.5.0.0.0, 14.6.0.0.0, 14.7.0.0.0
- Oracle BI Publisher, versions 7.0.0.0.0, 12.2.1.4.0
- Oracle Big Data Spatial et Graph, version 3.0.5
- Oracle Business Intelligence Enterprise Edition, versions 7.0.0.0.0, 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 et Revenue Management, versions 12.0.0.4-12.0.0.8, 15.0.0.0
- Oracle Communications BRM - Elastic Charging Engine, versions 12.0.0.4-12.0.0.8, 15.0.0.0
- Oracle Communications Cloud Native Core Binding Support Function, versions 23.4.0-23.4.2
- Oracle Communications Cloud Native Core Console, version 23.4.0
- Oracle Communications Cloud Native Core Network Data Analytics Function, version 24.1.0
- Oracle Communications Cloud Native Core Network Exposure Function, version 23.4.1
- Oracle Communications Cloud Native Core Network Function Cloud Native Environment, versions 23.2.0, 23.3.1, 23.4.0
- Oracle Communications Cloud Native Core Network Repository Function, version 23.4.1
- Oracle Communications Cloud Native Core Network Slice Selection Function, versions 23.2.0, 23.3.0
- Oracle Communications Cloud Native Core Policy, versions 23.4.0-23.4.2
- Oracle Communications Cloud Native Core Security Edge Protection Proxy, versions 23.3.0, 23.4.0
- Oracle Communications Cloud Native Core Service Communication Proxy, versions 23.1.0, 23.2.2, 23.3.0, 23.4.0
- Oracle Communications Cloud Native Core Unified Data Repository, versions 22.4.0, 23.1.0, 23.2.0, 23.3.2
- Oracle Communications Diameter Signaling Router, version 9.0.0.0

- Oracle Communications Element Manager, versions 9.0.0-9.0.2
- Oracle Communications Fraud Monitor, versions 5.0, 5.1, 5.2
- Oracle Communications Network Integrity, version 7.3.6.4
- Oracle Communications Offline Mediation Controller, versions 12.0.0.1-12.0.0.8
- Oracle Communications Operations Monitor, versions 5.0, 5.1, 5.2
- Oracle Communications Service Catalog et Design, version 8.0.0.1.0
- Oracle Communications Session Report Manager, versions 9.0.0-9.0.2
- Oracle Communications Unified Inventory Management, versions 7.4.0-7.4.2, 7.5.0, 7.5.1
- Oracle Communications User Data Repository, version 14.0.0.0.0
- Oracle Communications WebRTC Session Controller, versions 7.2.0.0.0-7.2.1.0.0
- Oracle Data Integrator, version 12.2.1.4.0
- Oracle Database Server, versions 19.3-19.22, 21.3-21.13
- Oracle Documaker, versions 12.6, 12.7
- Oracle E-Business Suite, versions 12.2.3-12.2.13
- Oracle Enterprise Data Quality, version 12.2.1.4.0
- Oracle Enterprise Manager Base Platform, version 13.5.0.0
- Oracle Enterprise Manager for Fusion Middleware, version 13.5.0.0
- Oracle Essbase, version 21.5.4.0.0
- Oracle Financial Services Revenue Management et Billing, versions 2.8.0.0.0, 2.9.0.0.0, 2.9.0.1.0, 3.0.0.0.0, 3.1.0.0.0, 3.2.0.0.0, 4.0.0.0, 5.0.0.0
- Oracle FLEXCUBE Private Banking, version 12.1.0.0.0
- Oracle Fusion Middleware MapViewer, version 12.2.1.4.0
- Oracle Global Lifecycle Management NextGen OUI Framework, version 12.2.1.4.0
- Oracle GoldenGate, versions 19.1.0.0.0-19.22.0.0.240124, 21.3-21.13
- Oracle GoldenGate Stream Analytics, versions 19.1.0.0.0-19.1.0.0.8
- Oracle GoldenGate Studio, version 12.2.0.4.0
- Oracle GoldenGate Veridata, versions 12.2.1.4.0-12.2.1.4.230922
- Oracle GraalVM Enterprise Edition, versions 20.3.13, 21.3.9
- Oracle GraalVM for JDK, versions 17.0.10, 21.0.2, 22
- Oracle Healthcare Data Repository, versions 8.1.0.0, 8.1.1.0, 8.1.2.0, 8.1.3.0, 8.1.3.2, 8.1.3.4
- Oracle Hospitality Cruise Shipboard Property Management System, versions 20.3.3, 20.3.4, 23.1.0, 23.1.1

- Oracle Hospitality Simphony, versions 19.1.0-19.5.4
- Oracle HTTP Server, versions 12.2.1.4.0, 14.1.1.0.0
- Oracle Hyperion Infrastructure Technology, version 11.2.16.0.0
- Oracle Identity Manager, version 12.2.1.4.0
- Oracle Identity Manager Connector, version 12.2.1.3.0
- Oracle Internet Directory, version 12.2.1.4.0
- Oracle Java SE, versions 8u401, 8u401-perf, 11.0.22, 17.0.10, 21.0.2, 22
- Oracle Life Sciences Empirica Signal, versions 9.1.0.53, 9.2.0.53
- Oracle Managed File Transfer, version 12.2.1.4.0
- Oracle Middleware Common Libraries et Tools, versions 12.2.1.4.0, 14.1.1.0.0
- Oracle Outside In Technology, versions 8.5.6, 8.5.7
- Oracle Retail Assortment Planning, versions 15.0.3, 16.0.3
- Oracle Retail Customer Management et Segmentation Foundation, version 19.0.0.9
- Oracle Retail Integration Bus, versions 14.1.3.2, 15.0.3.1, 16.0.3, 19.0.1
- Oracle Retail Merchandising System, versions 14.1.3, 15.0.3, 16.0.3, 19.0.1
- Oracle Retail Sales Audit, versions 14.1.3.1, 15.0.3.1, 16.0.3, 19.0.1
- Oracle Retail Service Backbone, versions 14.1.3.2, 15.0.3.1, 16.0.3, 19.0.1
- Oracle Retail Xstore Point of Service, versions 19.0.5, 20.0.4, 21.0.3, 22.0.1, 23.0.1
- Oracle SD-WAN Edge, version 9.1.1.7.0
- Oracle Smart View for Office, version 11.2.16.0.0
- Oracle SOA Suite, version 12.2.1.4.0
- Oracle Solaris, version 11
- Oracle Solaris Cluster, version 4
- Oracle StorageTek Tape Analytics (STA), version 2.5
- Oracle TimesTen In-Memory Database, versionsantérieure à 22.1,antérieure à 22.1.1.19.0,antérieure à 22.1.1.23.0
- Oracle Transportation Management, versions 6.5.2, 6.5.3
- Oracle Utilities Application Framework, versions 4.3.0.3.0-4.3.0.6.0, 4.4.0.0.0, 4.4.0.2.0, 4.4.0.3.0, 4.5.0.0.0, 4.5.0.1.1, 4.5.0.1.2
- Oracle Utilities Network Management System, versions 2.3.0.2, 2.4.0.1, 2.5.0.1, 2.5.0.2, 2.6.0.0, 2.6.0.0.4, 2.6.0.1
- Oracle VM VirtualBox, versionsantérieure à 7.0.16
- Oracle Web Services Manager, version 12.2.1.4.0
- Oracle WebCenter Content, version 12.2.1.4.0

- Oracle WebCenter Enterprise Capture, version 12.2.1.4.0
- Oracle WebCenter Portal, version 12.2.1.4.0
- Oracle WebLogic Server, versions 12.2.1.4.0, 14.1.1.0.0
- Oracle ZFS Storage Appliance Kit, version 8.8
- OSS Support Tools, versions 2.12.44, 2.12.45, 23.1.23.1.17, 24.1.24.1.16
- PeopleSoft Enterprise CRM Client Management, version 9.2
- PeopleSoft Enterprise HCM Benefits Administration, version 9.2
- PeopleSoft Enterprise PeopleTools, versions 8.59, 8.60, 8.61
- Primavera Gateway, versions 19.12.0-19.12.18, 20.12.0-20.12.13, 21.12.0-21.12.11
- Primavera P6 Enterprise Project Portfolio Management, versions 19.12.0-19.12.22, 20.12.0-20.12.21, 21.12.0-21.12.18, 22.12.0-22.12.12, 23.12.0-23.12.2
- Primavera Unifier, versions 19.12.0-19.12.16, 20.12.0-20.12.16, 21.12.0-21.12.17, 22.12.0-22.12.12, 23.12.0-23.12.3
- Siebel Applications, versions 24.2 et antérieure

Identificateurs externes

- CVE-2019-0231 CVE-2019-10172 CVE-2019-13990 CVE-2020-25638 CVE-2020-29508 CVE-2020-35163 CVE-2020-35164 CVE-2020-35166 CVE-2020-35167 CVE-2020-35168 CVE-2020-8908 CVE-2021-23369 CVE-2021-23383 CVE-2021-28861 CVE-2021-36373 CVE-2021-36374 CVE-2021-36770 CVE-2021-37533 CVE-2021-41616 CVE-2021-43113 CVE-2022-1471 CVE-2022-23491 CVE-2022-24329 CVE-2022-24613 CVE-2022-24614 CVE-2022-24839 CVE-2022-25147 CVE-2022-31160 CVE-2022-3171 CVE-2022-34169 CVE-2022-34381 CVE-2022-36033 CVE-2022-40152 CVE-2022-40896 CVE-2022-41704 CVE-2022-41853 CVE-2022-42003 CVE-2022-42004 CVE-2022-42889 CVE-2022-42890 CVE-2022-42920 CVE-2022-44729 CVE-2022-45378 CVE-2022-45688 CVE-2022-46337 CVE-2022-46364 CVE-2022-46751 CVE-2022-48579 CVE-2023-0464 CVE-2023-0465 CVE-2023-0466 CVE-2023-0833 CVE-2023-1108 CVE-2023-1255 CVE-2023-1370 CVE-2023-1436 CVE-2023-20860 CVE-2023-20861 CVE-2023-20862 CVE-2023-20863 CVE-2023-2283 CVE-2023-24021 CVE-2023-24998 CVE-2023-2617 CVE-2023-2618 CVE-2023-2650 CVE-2023-27391 CVE-2023-28708 CVE-2023-28823 CVE-2023-29081 CVE-2023-29499 CVE-2023-2975 CVE-2023-2976 CVE-2023-31122 CVE-2023-3223 CVE-2023-32611 CVE-2023-32636 CVE-2023-32643 CVE-2023-32665 CVE-2023-33201 CVE-2023-33202 CVE-2023-34034 CVE-2023-34035 CVE-2023-34053 CVE-2023-34055 CVE-2023-3446 CVE-2023-34981 CVE-2023-35116 CVE-2023-35141 CVE-2023-35887 CVE-2023-3635 CVE-2023-36478 CVE-2023-36479 CVE-2023-36632 CVE-2023-37536 CVE-2023-38039 CVE-2023-3817 CVE-2023-38325 CVE-2023-38545 CVE-2023-38546 CVE-2023-39151 CVE-2023-39975 CVE-2023-4016 CVE-2023-40167 CVE-2023-40217 CVE-2023-4043 CVE-2023-41056 CVE-2023-41074 CVE-2023-41080 CVE-2023-41105 CVE-2023-41900 CVE-2023-41993 CVE-2023-42282 CVE-2023-42503 CVE-2023-42917 CVE-2023-43494 CVE-2023-43495 CVE-2023-43496 CVE-2023-43497 CVE-2023-43498 CVE-2023-43622 CVE-2023-43804 CVE-2023-44271 CVE-2023-44483 CVE-2023-44487 CVE-2023-44981 CVE-2023-45142 CVE-

2023-4527 CVE-2023-45802 CVE-2023-45803 CVE-2023-46218 CVE-2023-46219 CVE-2023-46308 CVE-2023-4641 CVE-2023-46589 CVE-2023-46604 CVE-2023-46809 CVE-2023-47038 CVE-2023-47039 CVE-2023-47100 CVE-2023-4806 CVE-2023-4807 CVE-2023-4863 CVE-2023-48795 CVE-2023-49083 CVE-2023-4911 CVE-2023-50298 CVE-2023-50386 CVE-2023-5072 CVE-2023-50782 CVE-2023-51074 CVE-2023-51257 CVE-2023-5156 CVE-2023-51775 CVE-2023-52428 CVE-2023-5341 CVE-2023-5363 CVE-2023-5379 CVE-2023-5678 CVE-2023-5752 CVE-2023-6004 CVE-2023-6129 CVE-2023-6246 CVE-2023-6378 CVE-2023-6481 CVE-2023-6507 CVE-2023-6779 CVE-2023-6780 CVE-2023-6918 CVE-2024-0727 CVE-2024-0853 CVE-2024-1459 CVE-2024-1597 CVE-2024-1635 CVE-2024-20918 CVE-2024-20919 CVE-2024-20921 CVE-2024-20922 CVE-2024-20923 CVE-2024-20925 CVE-2024-20926 CVE-2024-20932 CVE-2024-20945 CVE-2024-20952 CVE-2024-20954 CVE-2024-20989 CVE-2024-20990 CVE-2024-20991 CVE-2024-20992 CVE-2024-20993 CVE-2024-20994 CVE-2024-20995 CVE-2024-20997 CVE-2024-20998 CVE-2024-20999 CVE-2024-21000 CVE-2024-21001 CVE-2024-21002 CVE-2024-21003 CVE-2024-21004 CVE-2024-21005 CVE-2024-21006 CVE-2024-21007 CVE-2024-21008 CVE-2024-21009 CVE-2024-21010 CVE-2024-21011 CVE-2024-21012 CVE-2024-21013 CVE-2024-21014 CVE-2024-21015 CVE-2024-21016 CVE-2024-21017 CVE-2024-21018 CVE-2024-21019 CVE-2024-21020 CVE-2024-21021 CVE-2024-21022 CVE-2024-21023 CVE-2024-21024 CVE-2024-21025 CVE-2024-21026 CVE-2024-21027 CVE-2024-21028 CVE-2024-21029 CVE-2024-21030 CVE-2024-21031 CVE-2024-21032 CVE-2024-21033 CVE-2024-21034 CVE-2024-21035 CVE-2024-21036 CVE-2024-21037 CVE-2024-21038 CVE-2024-21039 CVE-2024-21040 CVE-2024-21041 CVE-2024-21042 CVE-2024-21043 CVE-2024-21044 CVE-2024-21045 CVE-2024-21046 CVE-2024-21047 CVE-2024-21048 CVE-2024-21049 CVE-2024-21050 CVE-2024-21051 CVE-2024-21052 CVE-2024-21053 CVE-2024-21054 CVE-2024-21055 CVE-2024-21056 CVE-2024-21057 CVE-2024-21058 CVE-2024-21059 CVE-2024-21060 CVE-2024-21061 CVE-2024-21062 CVE-2024-21063 CVE-2024-21064 CVE-2024-21065 CVE-2024-21066 CVE-2024-21067 CVE-2024-21068 CVE-2024-21069 CVE-2024-21070 CVE-2024-21071 CVE-2024-21072 CVE-2024-21073 CVE-2024-21074 CVE-2024-21075 CVE-2024-21076 CVE-2024-21077 CVE-2024-21078 CVE-2024-21079 CVE-2024-21080 CVE-2024-21081 CVE-2024-21082 CVE-2024-21083 CVE-2024-21084 CVE-2024-21085 CVE-2024-21086 CVE-2024-21087 CVE-2024-21088 CVE-2024-21089 CVE-2024-21090 CVE-2024-21091 CVE-2024-21092 CVE-2024-21093 CVE-2024-21094 CVE-2024-21095 CVE-2024-21096 CVE-2024-21097 CVE-2024-21098 CVE-2024-21099 CVE-2024-21100 CVE-2024-21101 CVE-2024-21102 CVE-2024-21103 CVE-2024-21104 CVE-2024-21105 CVE-2024-21106 CVE-2024-21107 CVE-2024-21108 CVE-2024-21109 CVE-2024-21110 CVE-2024-21111 CVE-2024-21112 CVE-2024-21113 CVE-2024-21114 CVE-2024-21115 CVE-2024-21116 CVE-2024-21117 CVE-2024-21118 CVE-2024-21119 CVE-2024-21120 CVE-2024-21121 CVE-2024-21626 CVE-2024-21634 CVE-2024-21892 CVE-2024-22019 CVE-2024-22195 CVE-2024-22201 CVE-2024-22233 CVE-2024-22243 CVE-2024-22257 CVE-2024-22259 CVE-2024-23635 CVE-2024-23672 CVE-2024-24549 CVE-2024-24815 CVE-2024-24816 CVE-2024-25062 CVE-2024-25710 CVE-2024-26130 CVE-2024-26308

Bilan de la vulnérabilité

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Oracle a publié des correctifs de sécurité pour traiter plusieurs vulnérabilités critiques dans le cadre de sa mise à jour « Oracle Critical Patch Update » du mois Avril 2024. 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 16 Avril 2024, 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 16 Avril 2024**:**

- https://www.oracle.com/security-alerts/cpuapr2024.html

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma