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 Janvier 2024
Numéro de Référence	45661801/24
Date de Publication	18 Janvier 2024
Risque	Critique
Impact	Critique

Systèmes affectés

- JD Edwards EnterpriseOne Orchestrator, versions antérieure à 9.2.8.0
- JD Edwards EnterpriseOne Tools, versions antérieure à 9.2.8.1
- MySQL Cluster, versions 7.5.32 et antérieure, 7.6.28 et antérieure, 8.0.35 et antérieure, 8.1.0, 8.2.0 et antérieure
- MySQL Connectors, versions 8.0.35 et antérieure, 8.2.0 et antérieure
- MySQL Enterprise Monitor, versions 8.0.36 et antérieure
- MySQL Server, versions 8.0.35 et antérieure, 8.1.0, 8.2.0 et antérieure
- MySQL Workbench, versions 8.0.34 et antérieure
- Oracle Access Manager, version 12.2.1.4.0
- Oracle Agile PLM, version 9.3.6
- Oracle Agile Product Lifecycle Management pour Process, versions antérieure à 6.2.4.2
- Oracle Analytics Desktop, versions 6.4.0.0.0, antérieure à 7.2
- Oracle Application Testing Suite, version 13.3.0.1
- Oracle Audit Vault et Database Firewall, versions 20.1-20.9
- Oracle BI Publisher, versions 6.4.0.0.0, 7.0.0.0.0, 12.2.1.4.0
- Oracle Banking APIs, versions 19.1.0, 21.1.0, 22.1.0, 22.2.0
- Oracle Banking Branch, versions 14.5.0-14.7.0
- Oracle Banking Cash Management, versions 14.5.0-14.7.0
- Oracle Banking Collections et Recovery, versions 14.5.0-14.7.0
- Oracle Banking Corporate Lending Process Management, versions 14.5.0-14.7.0
- Oracle Banking Credit Facilities Process Management, versions 14.5.0-14.7.0

- Oracle Banking Digital Experience, versions 19.1.0, 21.1.0, 22.1.0, 22.2.0
- Oracle Banking Electronic Data Exchange pour Corporates, versions 14.5.0-14.7.0
- Oracle Banking Enterprise Default Management, versions 14.5.0-14.7.0
- Oracle Banking Extensibility Workbench, versions 14.5.0-14.7.0
- Oracle Banking Liquidity Management, versions 14.5.0-14.7.0, 14.7.0.3.0
- Oracle Banking Origination, versions 14.5.0-14.7.0
- Oracle Banking Party Management, versions 14.5.0-14.7.0
- Oracle Banking Supply Chain Finance, versions 14.5.0-14.7.0
- Oracle Banking Trade Finance Process Management, versions 14.5.0-14.7.0
- Oracle Banking Virtual Account Management, versions 14.5.0-14.7.0
- Oracle Big Data Spatial et Graph, version 3.0.4
- 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, version 11.3.2
- Oracle Communications ASAP, version 7.4
- Oracle Communications BRM - Elastic Charging Engine, versions 12.0.0.4 - 12.0.0.8
- Oracle Communications Billing et Revenue Management, versions 12.0.0.4 .0- 12.0.0.8 .0, 15.0.0.0.0
- Oracle Communications Cloud Native Core Automated Test Suite, versions 23.1.3, 23.2.1, 23.3.0
- Oracle Communications Cloud Native Core Console, versions 23.3.0, 23.3.1
- Oracle Communications Cloud Native Core Network Data Analytics Function, versions 23.3.0, 23.4.0
- Oracle Communications Cloud Native Core Network Exposure Function, version 23.3.1
- Oracle Communications Cloud Native Core Network Function Cloud Native Environment, versions 23.1.0, 23.2.0, 23.3.1
- Oracle Communications Cloud Native Core Network Repository Function, versions 23.1.4, 23.3.1
- Oracle Communications Cloud Native Core Network Slice Selection Function, versions 23.2.0, 23.3.1
- Oracle Communications Cloud Native Core Security Edge Protection Proxy, versions 23.1.0, 23.2.0, 23.3.0
- Oracle Communications Cloud Native Core Unified Data Repository, version 23.3.1

- Oracle Communications Convergence, versions 3.0.3.2 , 3.0.3.3
- Oracle Communications Convergent Charging Controller, versions 6.0.1.0.0, 12.0.1.0.0-12.0.6.0.0, 15.0.0.0.0
- Oracle Communications Diameter Signaling Router, versions 8.6.0.0 , 9.0.0.0
- Oracle Communications Element Manager, versions 9.0.0.0 .0-9.0.2.0.1, 9.4.53
- Oracle Communications Fraud Monitor, versions 5.0, 5.1
- Oracle Communications IP Service Activator, versions 7.4.0, 7.5.0
- Oracle Communications Instant Messaging Server, version 10.0.1.7.0
- Oracle Communications Messaging Server, version 8.1.0.24.0
- Oracle Communications MetaSolv Solution, version 6.3.1.0.0
- Oracle Communications Network Analytics Data Director, versions 23.2.0.0.2, 23.3.0.0.0
- Oracle Communications Network Charging et Control, versions 6.0.1.0.0, 12.0.1.0.0-12.0.6.0.0, 15.0.0.0.0
- Oracle Communications Order et Service Management, versions 7.4.0, 7.4.1
- Oracle Communications Policy Management, versions 12.6.1.0.0, 15.0.0.0.0
- Oracle Communications Pricing Design Center, versions 12.0.0.4 .0- 12.0.0.8 .0, 15.0.0.0.0
- Oracle Communications Service Catalog et Design, versions 7.4.0.7.0, 7.4.1.5.0, 7.4.2.8.0
- Oracle Communications Session Report Manager, versions 9.0.0.0 .0-9.0.2.0.1, 9.4.53
- Oracle Communications Unified Assurance, versions 5.0.0-5.5.19, 6.0.0-6.0.3
- Oracle Communications Unified Inventory Management, versions 7.4.0, 7.4.1, 7.4.2
- Oracle Complex Maintenance, Repair, et Overhaul, versions 11.5, 12.1, 12.2
- Oracle Database Server, versions 19.3-19.21, 21.3-21.12, 22.3-23.8, 23.9.0-23.9.4, 23.10
- 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 Ops Center, version 12.4.0.0
- Oracle Enterprise Manager pour Fusion Middleware, version 13.5.0.0
- Oracle Enterprise Manager pour Oracle Database, version 13.5.0.0
- Oracle Enterprise Manager pour Oracle Virtual Infrastructure, version 13.5.0.0
- Oracle Enterprise Manager pour Virtualization, version 13.5.0.0
- Oracle Essbase, version 21.5.3.0.0
- Oracle FLEXCUBE Enterprise Limits et Collateral Management, versions 14.5.0-14.7.0

- Oracle FLEXCUBE Investor Servicing, versions 14.5.0-14.7.0
- Oracle FLEXCUBE Private Banking, versions 14.5.0-14.7.0
- Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.7, 8.0.8, 8.0.9, 8.1.0, 8.1.1, 8.1.2
- Oracle Financial Services Behavior Detection Platform, versions 8.0.8.1 , 8.1.1.1 , 8.1.2.5 , 8.1.2.6
- Oracle Financial Services Compliance Studio, version 8.1.2.5
- Oracle Financial Services Enterprise Case Management, versions 8.0.8.2 , 8.1.1.1 , 8.1.2.5 , 8.1.2.6
- Oracle Financial Services Lending et Leasing, versions 14.5.0-14.7.0
- Oracle Financial Services Revenue Management et Billing, versions 2.7.1, 2.8.0, 2.9.0, 2.9.1, 3.0.0-3.2.0, 4.0.0, 5.0.0, 5.1.0, 6.0.0
- Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition, version 8.0.8
- Oracle Fusion Middleware, version 12.2.1.4.0
- Oracle Global Lifecycle Management OPatch, versions antérieure à 12.2.0.1.40
- Oracle GoldenGate Studio, version 12.2.0.4.0
- Oracle GoldenGate, versions 19.1.0.0.0-19.1.0.0.231017, 21.3-21.12
- Oracle GraalVM Enterprise Edition, versions 20.3.12, 21.3.8, 22.3.4
- Oracle GraalVM pour JDK, versions 17.0.9, 21.0.1
- Oracle Graph Server et Client, versions antérieure à 22.4.6, antérieure à 23.4.0
- Oracle HTTP Server, version 12.2.1.4.0
- Oracle Hyperion Calculation Manager, version 11.2.14.0.0
- Oracle Hyperion Financial Data Quality Management, Enterprise Edition, version 11.2.14.0.0
- Oracle Hyperion Financial Management, version 11.2.14.0.0
- Oracle Hyperion Financial Reporting, version 11.2.14.0.0
- Oracle Hyperion Infrastructure Technology, version 11.2.14.0.0
- Oracle Hyperion Planning, version 11.2.14.0.0
- Oracle Identity Manager, version 12.2.1.4.0
- Oracle JDeveloper, version 12.2.1.4.0
- Oracle Java SE, versions 8u391, 8u391-perf, 11.0.21, 17.0.9, 21.0.1
- Oracle Managed File Transfer, version 12.2.1.4.0
- Oracle Middleware Common Libraries et Tools, version 12.2.1.4.0

- Oracle NoSQL Database, versions antérieure à 1.6, antérieure à 19.5.40, antérieure à 20.3.38, antérieure à 21.2.30, antérieure à 22.3.94, antérieure à 23.1.29
- Oracle Outside In Technology, version 8.5.6
- Oracle REST Data Services, versions antérieure à 23.3.0
- Oracle Retail Advanced Inventory Planning, versions 15.0.3, 16.0.3
- Oracle Retail Customer Management et Segmentation Foundation, versions 18.0.0.14 , 19.0.0.8
- Oracle Retail EFTLink, versions 20.0.1, 21.0.0-23.0.0
- Oracle SOA Suite, version 12.2.1.4.0
- Oracle SQL Developer, versions 21.4.2, 22.2.0, 23.1.0
- Oracle Secure Backup, versions antérieure à 18.1.0.2.0
- Oracle Service Bus, version 12.2.1.4.0
- Oracle Solaris, version 11
- 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 , 2.6.0.1
- Oracle Utilties 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, 4.5.0.1.3
- Oracle WebCenter Content, version 12.2.1.4.0
- Oracle WebCenter Portal, version 12.2.1.4.0
- Oracle WebCenter Sites, version 12.2.1.4.0
- Oracle WebLogic Server, versions 12.2.1.4.0, 14.1.1.0.0
- Oracle ZFS Storage Appliance Kit, version 8.8
- PeopleSoft Enterprise PeopleTools, versions 8.59, 8.60, 8.61
- Primavera P6 Enterprise Project Portfolio Management, versions 19.12.0-19.12.22, 20.12.0-20.12.20, 21.12.0-21.12.17, 22.12.0-22.12.10
- Primavera Unifier, versions 19.12.0-19.12.16, 20.12.0-20.12.16, 21.12.0-21.12.17, 22.12.0-22.12.11
- Siebel Applications, versions antérieure à 23.12
- TimesTen In-Memory Database, versions antérieure à 21.1.1.19.0, antérieure à 22.1.1.19.0
- Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers, versions antérieure à XCP2430, antérieure à XCP3130, antérieure à XCP4040
- GoldenGate Big Data et Application Adapters, versions 19.1.0.0.0-19.1.0.0.16, 21.3-21.12
- Integrated Lights Out Manager (ILOM), versions 3, 4, 5

Identificateurs externes

- CVE-2019-10086 CVE-2020-15250 CVE-2020-26870 CVE-2020-29508 CVE-2020-35163 CVE-2020-35164 CVE-2020-35166 CVE-2020-35167 CVE-2020-35168 CVE-2020-5410 CVE-2020-5421 CVE-2020-7760 CVE-2021-0341 CVE-2021-29425 CVE-2021-33813 CVE-2021-35515 CVE-2021-35516 CVE-2021-35517 CVE-2021-36090 CVE-2021-37533 CVE-2021-4104 CVE-2021-41182 CVE-2021-41183 CVE-2021-41184 CVE-2021-42392 CVE-2021-42575 CVE-2021-43306 CVE-2021-43527 CVE-2021-46848 CVE-2022-1471 CVE-2022-21432 CVE-2022-22950 CVE-2022-22969 CVE-2022-22979 CVE-2022-23221 CVE-2022-24839 CVE-2022-25147 CVE-2022-25647 CVE-2022-29155 CVE-2022-31147 CVE-2022-31160 CVE-2022-31690 CVE-2022-31692 CVE-2022-33879 CVE-2022-34169 CVE-2022-3479 CVE-2022-3510 CVE-2022-3602 CVE-2022-36033 CVE-2022-36944 CVE-2022-37434 CVE-2022-3786 CVE-2022-40152 CVE-2022-40896 CVE-2022-41409 CVE-2022-41704 CVE-2022-42003 CVE-2022-42004 CVE-2022-42889 CVE-2022-42890 CVE-2022-42920 CVE-2022-4304 CVE-2022-4450 CVE-2022-44729 CVE-2022-44730 CVE-2022-45868 CVE-2022-46337 CVE-2022-46751 CVE-2022-46908 CVE-2022-48174 CVE-2023-0464 CVE-2023-0465 CVE-2023-0466 CVE-2023-1108 CVE-2023-1370 CVE-2023-1436 CVE-2023-20863 CVE-2023-20883 CVE-2023-21833 CVE-2023-21901 CVE-2023-21949 CVE-2023-22102 CVE-2023-2283 CVE-2023-23931 CVE-2023-24998 CVE-2023-25194 CVE-2023-2617 CVE-2023-2618 CVE-2023-2650 CVE-2023-27391 CVE-2023-28439 CVE-2023-28484 CVE-2023-28755 CVE-2023-28756 CVE-2023-28823 CVE-2023-29469 CVE-2023-2975 CVE-2023-2976 CVE-2023-30861 CVE-2023-31122 CVE-2023-31484 CVE-2023-31486 CVE-2023-31582 CVE-2023-32002 CVE-2023-32006 CVE-2023-32559 CVE-2023-32697 CVE-2023-33201 CVE-2023-34034 CVE-2023-34035 CVE-2023-34053 CVE-2023-34055 CVE-2023-34453 CVE-2023-34454 CVE-2023-34455 CVE-2023-3446 CVE-2023-34462 CVE-2023-34624 CVE-2023-34981 CVE-2023-35141 CVE-2023-35887 CVE-2023-36054 CVE-2023-3635 CVE-2023-36478 CVE-2023-36479 CVE-2023-36632 CVE-2023-37536 CVE-2023-38039 CVE-2023-3817 CVE-2023-3823 CVE-2023-3824 CVE-2023-38325 CVE-2023-38545 CVE-2023-38546 CVE-2023-39151 CVE-2023-39318 CVE-2023-39319 CVE-2023-39320 CVE-2023-39321 CVE-2023-39322 CVE-2023-39410 CVE-2023-39975 CVE-2023-40167 CVE-2023-4043 CVE-2023-41053 CVE-2023-41105 CVE-2023-41900 CVE-2023-42503 CVE-2023-42794 CVE-2023-42795 CVE-2023-43494 CVE-2023-43495 CVE-2023-43496 CVE-2023-43497 CVE-2023-43498 CVE-2023-43622 CVE-2023-43642 CVE-2023-43643 CVE-2023-44483 CVE-2023-44487 CVE-2023-44981 CVE-2023-45143 CVE-2023-45145 CVE-2023-45648 CVE-2023-45802 CVE-2023-46589 CVE-2023-46604 CVE-2023-47248 CVE-2023-48795 CVE-2023-49093 CVE-2023-4911 CVE-2023-50164 CVE-2023-5072 CVE-2023-5363 CVE-2024-20903 CVE-2024-20904 CVE-2024-20905 CVE-2024-20906 CVE-2024-20907 CVE-2024-20908 CVE-2024-20909 CVE-2024-20910 CVE-2024-20911 CVE-2024-20912 CVE-2024-20913 CVE-2024-20914 CVE-2024-20915 CVE-2024-20916 CVE-2024-20917 CVE-2024-20918 CVE-2024-20919 CVE-2024-20920 CVE-2024-20921 CVE-2024-20922 CVE-2024-20923 CVE-2024-20924 CVE-2024-20925 CVE-2024-20926 CVE-2024-20927 CVE-2024-20928 CVE-2024-20929 CVE-2024-20930 CVE-2024-20931 CVE-2024-20932 CVE-2024-20933 CVE-2024-20934 CVE-2024-20935 CVE-2024-20936 CVE-2024-20937 CVE-2024-20938 CVE-2024-20939 CVE-2024-20940 CVE-2024-20941 CVE-2024-20942 CVE-2024-20943 CVE-2024-20944 CVE-2024-20945 CVE-2024-20946 CVE-2024-20947 CVE-2024-20948 CVE-2024-20949

CVE-2024-20950 CVE-2024-20951 CVE-2024-20952 CVE-2024-20953 CVE-2024-20955 CVE-2024-20956 CVE-2024-20957 CVE-2024-20958 CVE-2024-20959 CVE-2024-20960 CVE-2024-20961 CVE-2024-20962 CVE-2024-20963 CVE-2024-20964 CVE-2024-20965 CVE-2024-20966 CVE-2024-20967 CVE-2024-20968 CVE-2024-20969 CVE-2024-20970 CVE-2024-20971 CVE-2024-20972 CVE-2024-20973 CVE-2024-20974 CVE-2024-20975 CVE-2024-20976 CVE-2024-20977 CVE-2024-20978 CVE-2024-20979 CVE-2024-20980 CVE-2024-20981 CVE-2024-20982 CVE-2024-20983 CVE-2024-20984 CVE-2024-20985 CVE-2024-20986 CVE-2024-20987

Bilan de la vulnérabilité

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 Janvier 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 Janvier 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 Janvier 2024**:**

- https://www.oracle.com/security-alerts/cpujan2024.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