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	48431807/24
Date de Publication	18 Juillet 2024
Risque	Important
Impact	Critique

Systèmes affectés

- JD Edwards EnterpriseOne Orchestrator, versions prior to 9.2.8.3
- JD Edwards EnterpriseOne Tools, versions prior to 9.2.8.2
- JD Edwards World Security, version A9.4
- Management Pack for Oracle GoldenGate, version 12.2.1.2
- MySQL Cluster, versions 7.5.34 and prior, 7.6.30 and prior, 8.0.37 and prior, 8.1.0 and prior, 8.3.0 and prior, 8.4.0 and prior
- MySQL Connectors, versions 8.4.0 and prior
- MySQL Enterprise Monitor, versions 8.0.38 and prior
- MySQL Server, versions 8.0.37 and prior, 8.0.38, 8.2.0 and prior, 8.3.0 and prior, 8.4.0 and prior, 8.4.1, 9.0.0
- MySQL Workbench, versions 8.0.36 and prior
- Oracle Access Manager, version 12.2.1.4.0
- Oracle Agile Engineering Data Management, versions 6.2.1.0-6.2.1.9
- Oracle Analytics Desktop, versions prior to 7.7.0, prior to 7.8.0
- Oracle Application Express, version 23.2
- Oracle Application Testing Suite, version 13.3.0.1
- Oracle Autovue for Agile Product Lifecycle Management, version 21.0.2
- Oracle Banking Branch, versions 14.4.0.0.0, 14.5.0.0.0, 14.6.0.0.0, 14.7.0.0.0
- Oracle Banking Cash Management, versions 14.4.0.0.0, 14.5.0.0.0, 14.6.0.0.0, 14.7.0.0.0
- Oracle Banking Corporate Lending Process Management, versions 14.4.0.0.0, 14.5.0.0.0, 14.6.0.0.0, 14.7.0.0.0
- Oracle Banking Credit Facilities Process Management, versions 14.5.0.0.0, 14.6.0.0.0, 14.7.0.0.0
- Oracle Banking Deposits and Lines of Credit Servicing, version 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
- 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, version 2.4.0.0.0
- Oracle Banking Virtual Account Management, versions 14.5.0.0.0, 14.6.0.0.0, 14.7.0.0.0
- Oracle Big Data Spatial and Graph, version 3.0.6
- Oracle Business Activity Monitoring, version 12.2.1.4.0
- Oracle Business Intelligence Enterprise Edition, versions 7.0.0.0.0, 7.6.0.0.0, 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 ASAP, version 7.4
- Oracle Communications Billing and Revenue Management, versions 12.0.0.4.0-12.0.0.8.0, 15.0.0.0.0
- Oracle Communications BRM - Elastic Charging Engine, versions 12.0.0.4-12.0.0.8, 15.0.0.0
- Oracle Communications Cloud Native Core Automated Test Suite, versions 23.1.0, 23.4.0
- Oracle Communications Cloud Native Core Binding Support Function, versions 23.4.0-23.4.3
- Oracle Communications Cloud Native Core Console, versions 23.4.0, 23.4.1
- Oracle Communications Cloud Native Core Network Data Analytics Function, version 24.2.0
- Oracle Communications Cloud Native Core Network Exposure Function, version 23.4.3
- Oracle Communications Cloud Native Core Network Function Cloud Native Environment, versions 23.4.0, 24.1.0
- Oracle Communications Cloud Native Core Network Repository Function, version 23.4.2
- Oracle Communications Cloud Native Core Policy, versions 23.4.0-23.4.4
- Oracle Communications Cloud Native Core Security Edge Protection Proxy, versions 23.4.0, 24.1.0
- Oracle Communications Cloud Native Core Service Communication Proxy, versions 23.4.0, 23.4.1, 23.4.2, 24.1.0
- Oracle Communications Cloud Native Core Unified Data Repository, versions 23.4.1, 23.4.2
- Oracle Communications Converged Charging System, versions 2.0.0.0.0, 2.0.0.1.0
- 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 8.6.0.4-8.6.0.8
- Oracle Communications EAGLE Element Management System, versions 46.6.4, 46.6.5
- Oracle Communications Element Manager, versions 9.0.0-9.0.3
- Oracle Communications Network Analytics Data Director, versions 23.4.0, 24.1.0
- Oracle Communications Network Charging and Control, versions 6.0.1.0.0, 12.0.1.0.0-12.0.6.0.0, 15.0.0.0.0
- Oracle Communications Operations Monitor, versions 5.1, 5.2
- Oracle Communications Performance Intelligence, version 10.5
- 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 and Design, versions 7.4.0-7.4.2, 8.0.0
- Oracle Communications Session Border Controller, versions 4.1.0, 4.2.0, 9.2.0, 9.3.0
- Oracle Communications Session Report Manager, versions 9.0.0-9.0.3
- Oracle Communications Unified Assurance, versions 5.5.0-5.5.21, 6.0.0-6.0.4
- Oracle Communications Unified Inventory Management, versions 7.4.1, 7.4.2
- Oracle Communications User Data Repository, versions 12.11.0, 12.11.3, 12.11.4
- Oracle Data Integrator, version 12.2.1.4.0
- Oracle Database Server, versions 19.3-19.23, 21.3-21.14, 23.4
- Oracle Documaker, versions 12.6.4, 12.7.1
- 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 Essbase, version 21.5.6
- Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.7, 8.0.8, 8.1.1, 8.1.2
- Oracle Financial Services Basel Regulatory Capital Basic, versions 8.0.7.3, 8.0.8.3
- Oracle Financial Services Basel Regulatory Capital Internal Ratings Based Approach, versions 8.0.7.3, 8.0.8.3
- Oracle Financial Services Behavior Detection Platform, versions 8.0.8.1, 8.1.1.1, 8.1.2.6, 8.1.2.7
- Oracle Financial Services Compliance Studio, versions 8.1.2.6, 8.1.2.7
- Oracle Financial Services Enterprise Case Management, versions 8.0.8.2.8, 8.1.1.1.18, 8.1.2.6.4, 8.1.2.7.3
- Oracle Financial Services Model Management and Governance, versions 8.1.2.5, 8.1.2.6
- Oracle Financial Services Revenue Management and Billing, versions 6.0.0.0.0, 6.1.0.0.0
- Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition, version 8.0.8.0
- Oracle FLEXCUBE Investor Servicing, versions 14.5.0.0.0, 14.7.0.0.0
- Oracle FLEXCUBE Universal Banking, versions 14.5.0.0.0, 14.6.0.0.0, 14.7.0.0.0
- Oracle Fusion Middleware, version 12.2.1.4.0
- Oracle Global Lifecycle Management NextGen OUI Framework, version 12.2.1.4.0
- Oracle GoldenGate, versions 19.1.0.0.0-19.23.0.0.240716, 21.3-21.14
- Oracle GoldenGate Big Data and Application Adapters, versions 19.1.0.0.0-19.1.0.0.18, 21.3-21.14.0.0.0
- Oracle GoldenGate Studio, version 12.2.0.4.0
- Oracle GraalVM Enterprise Edition, versions 20.3.14, 21.3.10
- Oracle GraalVM for JDK, versions 17.0.11, 21.0.3, 22.0.1
- Oracle Graph Server and Client, versions 22.4.7 and prior, 23.4.2 and prior, 24.1.0 and prior
- Oracle Healthcare Data Repository, versions 8.1.4, 8.2.0
- Oracle Healthcare Foundation, versions 8.2.0, 8.2.1, 8.2.2, 8.2.3, 8.2.4
- Oracle Healthcare Master Person Index, versions 5.0.0-5.0.9
- Oracle HTTP Server, version 12.2.1.4.0
- Oracle Hyperion Data Relationship Management, version 11.2.17.0.0
- Oracle Hyperion Financial Close Management, version 11.2.17.0.0
- Oracle Hyperion Infrastructure Technology, version 11.2.17.0.0
- Oracle Identity Manager, version 12.2.1.4.0
- Oracle Insurance Policy Administration J2EE, versions 11.2.12, 11.3.0-11.3.2
- Oracle Java SE, versions 8u411, 8u411-perf, 11.0.23, 17.0.11, 21.0.3, 22.0.1
- Oracle JDeveloper, version 12.2.1.4.0
- Oracle Middleware Common Libraries and Tools, version 12.2.1.4.0
- Oracle NoSQL Database, versions 1.4, 1.5, prior to 19.5.42, prior to 20.3.40, prior to 21.2.27, prior to 22.3.46, prior to 23.3.32
- Oracle Outside In Technology, version 8.5.7
- Oracle Reports Developer, versions 12.2.1.4.0, 12.2.1.19.0
- Oracle REST Data Services, versions prior to 23.3.1, prior to 24.1.0
- Oracle Retail Assortment Planning, versions 15.0.3, 16.0.3
- 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 Predictive Application Server, versions 15.0.3, 16.0.3
- Oracle Retail Xstore Office, versions 19.0.5, 20.0.3, 20.0.4, 22.0.0, 23.0.1
- Oracle Service Bus, version 12.2.1.4.0
- Oracle Solaris, version 11
- Oracle TimesTen In-Memory Database, versions 22.1.1.1.0-22.1.1.24.0

- Oracle Unified Directory, version 12.2.1.4.0
- Oracle Utilities Application Framework, versions 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, 24.1.0.0.0, 24.2.0.0.0
- Oracle VM VirtualBox, versions prior to 7.0.20
- 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 HCM Human Resources, version 9.2
- PeopleSoft Enterprise HCM Shared Components, version 9.2
- PeopleSoft Enterprise PeopleTools, versions 8.59, 8.60, 8.61
- Primavera Gateway, versions 19.12.0-19.12.19, 20.12.0-20.12.14, 21.12.0-21.12.12
- Primavera Unifier, versions 19.12.0-19.12.16, 20.12.0-20.12.16, 21.12.0-21.12.17, 22.12.0-22.12.13, 23.12.0-23.12.6
- Siebel Applications, versions 22.12 and prior, 23.12 and prior, 24.6 and prior

Identificateurs externes

CVE-2019-10086 CVE-2019-13990 CVE-2019-17267 CVE-2020-11987 CVE-2020-13956
CVE-2020-1945 CVE-2021-23926 CVE-2021-24112 CVE-2021-27568 CVE-2021-29425
CVE-2021-29489 CVE-2021-36090 CVE-2021-36373 CVE-2021-36374 CVE-2021-37533
CVE-2021-41182 CVE-2021-41183 CVE-2021-41184 CVE-2021-44550 CVE-2022-0239
CVE-2022-1292 CVE-2022-21797 CVE-2022-22950 CVE-2022-22965 CVE-2022-22968
CVE-2022-22970 CVE-2022-25987 CVE-2022-31160 CVE-2022-33879 CVE-2022-34169
CVE-2022-34381 CVE-2022-36033 CVE-2022-36944 CVE-2022-37434 CVE-2022-3786
CVE-2022-38398 CVE-2022-38648 CVE-2022-40146 CVE-2022-40149 CVE-2022-40150
CVE-2022-40152 CVE-2022-41704 CVE-2022-41881 CVE-2022-41915 CVE-2022-42003
CVE-2022-42890 CVE-2022-45378 CVE-2022-45685 CVE-2022-45693 CVE-2022-46337
CVE-2022-48174 CVE-2023-1370 CVE-2023-1436 CVE-2023-20861 CVE-2023-21036
CVE-2023-22081 CVE-2023-24998 CVE-2023-26031 CVE-2023-28755 CVE-2023-28756
CVE-2023-29081 CVE-2023-2975 CVE-2023-2976 CVE-2023-33201 CVE-2023-33202
CVE-2023-34034 CVE-2023-34040 CVE-2023-34055 CVE-2023-3446 CVE-2023-35116
CVE-2023-35887 CVE-2023-36478 CVE-2023-36479 CVE-2023-37536 CVE-2023-37920
CVE-2023-3817 CVE-2023-38552 CVE-2023-38709 CVE-2023-39331 CVE-2023-39332
CVE-2023-40167 CVE-2023-4043 CVE-2023-40743 CVE-2023-41105 CVE-2023-41900
CVE-2023-42503 CVE-2023-44483 CVE-2023-44487 CVE-2023-45853 CVE-2023-46218
CVE-2023-46219 CVE-2023-46589 CVE-2023-46750 CVE-2023-47248 CVE-2023-4759
CVE-2023-47627 CVE-2023-48795 CVE-2023-49081 CVE-2023-49082 CVE-2023-49083
CVE-2023-50447 CVE-2023-5072 CVE-2023-51074 CVE-2023-51775 CVE-2023-52425
CVE-2023-52426 CVE-2023-52428 CVE-2023-5363 CVE-2023-5678 CVE-2023-5685
CVE-2023-5764 CVE-2023-5981 CVE-2023-6004 CVE-2023-6129 CVE-2023-6597
CVE-2023-6918 CVE-2024-0232 CVE-2024-0397 CVE-2024-0450 CVE-2024-0727
CVE-2024-0853 CVE-2024-20996 CVE-2024-21098 CVE-2024-21122 CVE-2024-21123
CVE-2024-21125 CVE-2024-21126 CVE-2024-21127 CVE-2024-21128 CVE-2024-21129
CVE-2024-21130 CVE-2024-21131 CVE-2024-21132 CVE-2024-21133 CVE-2024-21134
CVE-2024-21135 CVE-2024-21136 CVE-2024-21137 CVE-2024-21138 CVE-2024-21139

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
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
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

CVE-2024-21140 CVE-2024-21141 CVE-2024-21142 CVE-2024-21143 CVE-2024-21144
CVE-2024-21145 CVE-2024-21146 CVE-2024-21147 CVE-2024-21148 CVE-2024-21149
CVE-2024-21150 CVE-2024-21151 CVE-2024-21152 CVE-2024-21153 CVE-2024-21154
CVE-2024-21155 CVE-2024-21157 CVE-2024-21158 CVE-2024-21159 CVE-2024-21160
CVE-2024-21161 CVE-2024-21162 CVE-2024-21163 CVE-2024-21164 CVE-2024-21165
CVE-2024-21166 CVE-2024-21167 CVE-2024-21168 CVE-2024-21169 CVE-2024-21170
CVE-2024-21171 CVE-2024-21173 CVE-2024-21174 CVE-2024-21175 CVE-2024-21176
CVE-2024-21177 CVE-2024-21178 CVE-2024-21179 CVE-2024-21180 CVE-2024-21181
CVE-2024-21182 CVE-2024-21183 CVE-2024-21184 CVE-2024-21185 CVE-2024-21188
CVE-2024-21742 CVE-2024-21892 CVE-2024-22019 CVE-2024-22025 CVE-2024-22201
CVE-2024-22234 CVE-2024-22243 CVE-2024-22257 CVE-2024-22259 CVE-2024-22262
CVE-2024-23635 CVE-2024-23672 CVE-2024-23807 CVE-2024-23897 CVE-2024-23898
CVE-2024-23944 CVE-2024-24549 CVE-2024-24795 CVE-2024-24815 CVE-2024-24816
CVE-2024-25062 CVE-2024-2511 CVE-2024-25710 CVE-2024-26130 CVE-2024-26308
CVE-2024-27316 CVE-2024-27980 CVE-2024-27982 CVE-2024-27983 CVE-2024-28182
CVE-2024-28752 CVE-2024-28757 CVE-2024-28849 CVE-2024-29025 CVE-2024-29041
CVE-2024-29131 CVE-2024-29133 CVE-2024-29203 CVE-2024-2961 CVE-2024-29857
CVE-2024-29881 CVE-2024-30171 CVE-2024-30172 CVE-2024-32114 CVE-2024-34064
CVE-2024-34069 CVE-2024-34447 CVE-2024-34459 CVE-2024-4603 CVE-2024-4741
CVE-2024-6162

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

Bulletin de sécurité d’Oracle :

- https://www.oracle.com/security-alerts/cpujul2024.html#AppendixFMW

Direction Générale de la Sécurité des Systèmes d’Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
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
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma