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	44401910/23
Date de Publication	19 Octobre 2023
Risque	Important
Impact	Critique

Systèmes affectés

- BI Publisher, versions 6.4.0.0.0, 7.0.0.0.0, 12.2.1.4.0
- GoldenGate Big Data, versions 21.3-21.10
- GoldenGate Veridata, versions 12.2.1.4.0-12.2.1.4.230922
- Hospitality OPERA 5 Property Services, version 5.6
- JD Edwards EnterpriseOne Tools, version 9.2.7
- Management Cloud Engine, version 23.1.0.0
- MySQL Cluster, versions 8.0.34 and prior, 8.1.0
- MySQL Connectors, versions 8.1.0 and prior
- MySQL Enterprise Monitor, versions 8.0.35 and prior
- MySQL Installer, versions prior to 1.6.8
- MySQL Server, versions 5.7.43 and prior, 8.0.34 and prior, 8.1.0 and prior
- MySQL Shell, versions 8.1.1 and prior
- 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 Banking APIs, versions 18.3, 19.1, 19.2, 21.1, 22.1, 22.2
- Oracle Banking Branch, versions 14.5-14.7
- Oracle Banking Cash Management, versions 14.5-14.7
- Oracle Banking Corporate Lending, versions 14.0-14.3, 14.5-14.7
- Oracle Banking Corporate Lending Process Management, versions 14.5-14.7
- Oracle Banking Credit Facilities Process Management, versions 14.5-14.7
- Oracle Banking Deposits and Lines of Credit Servicing, versions 2.7, 2.12
- Oracle Banking Digital Experience, versions 18.3, 19.1, 19.2, 21.1, 22.1, 22.2
- Oracle Banking Electronic Data Exchange for Corporates, versions 14.5-14.7
- Oracle Banking Liquidity Management, versions 14.5-14.7
- Oracle Banking Loans Servicing, version 2.12

- Oracle Banking Origination, versions 14.5-14.7
- Oracle Banking Party Management, version 2.7
- Oracle Banking Payments, versions 14.0-14.3, 14.5-14.7
- Oracle Banking Platform, versions 2.6.2, 2.9.0
- Oracle Banking Supply Chain Finance, versions 14.5-14.7
- Oracle Banking Trade Finance, versions 14.5-14.7
- Oracle Banking Trade Finance Process Management, versions 14.5-14.7
- Oracle Banking Virtual Account Management, versions 14.5-14.7
- Oracle Big Data Spatial and Graph, versions 2.5 and prior
- 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 Communications BRM - Elastic Charging Engine, versions 12.0.0.4-12.0.0.8
- Oracle Communications Cloud Native Core Binding Support Function, versions 23.1.0-23.1.8, 23.2.0-23.2.4
- Oracle Communications Cloud Native Core Console, versions 23.1.1, 23.1.2, 23.2.1
- Oracle Communications Cloud Native Core Network Exposure Function, versions 23.1.3, 23.3.0
- Oracle Communications Cloud Native Core Network Function Cloud Native Environment, versions 23.2.0, 23.2.2
- Oracle Communications Cloud Native Core Network Repository Function, versions 23.1.3, 23.2.1, 23.3.0
- Oracle Communications Cloud Native Core Policy, versions 23.1.0-23.1.8, 23.2.0-23.2.4
- Oracle Communications Cloud Native Core Security Edge Protection Proxy, versions 23.1.0, 23.1.3, 23.3.0
- Oracle Communications Cloud Native Core Unified Data Repository, version 23.1.2
- Oracle Communications Convergent Charging Controller, version 12.0.6.0
- Oracle Communications Diameter Signaling Router, versions 8.6.0.0, 9.0.0.0
- Oracle Communications Element Manager, versions 9.0.0-9.0.2
- Oracle Communications IP Service Activator, versions 7.4.0, 7.5.0
- Oracle Communications MetaSolv Solution, version 6.3.1.0.0
- Oracle Communications Network Analytics Data Director, version 23.2.0
- Oracle Communications Network Charging and Control, version 12.0.6.0
- Oracle Communications Order and Service Management, versions 7.4.0, 7.4.1
- Oracle Communications Policy Management, version 12.6.0.0
- Oracle Communications Session Report Manager, versions 9.0.0-9.0.2
- Oracle Communications Unified Assurance, versions 5.5.0-5.5.17, 6.0.0-6.0.3
- 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 19.3-19.20, 21.3-21.11
- Oracle Documaker, versions 12.6.4-12.7.1
- Oracle E-Business Suite, versions 12.2.3-12.2.12, [ECC] 8, [ECC] 9, [ECC] 10
- Oracle Enterprise Communications Broker, versions 3.3, 4.0, 4.1
- Oracle Enterprise Data Quality, version 12.2.1.4.0
- Oracle Enterprise Manager Base Platform, version 13.5.0.0
- Oracle Enterprise Manager for Peoplesoft, version 13.5.1.1
- Oracle Enterprise Manager Ops Center, version 12.4.0.0
- Oracle Enterprise Operations Monitor, versions 5.0, 5.1
- Oracle Enterprise Session Border Controller, versions 9.0-9.2

- Oracle Essbase, version 21.5.0.0.0
- Oracle Financial Services Cash Flow Engine, version 8.1.2.0.0
- Oracle Financial Services Model Management and Governance, versions 8.1.2.3, 8.1.2.4
- Oracle FLEXCUBE Core Banking, versions 11.6-11.8, 11.10, 11.11
- Oracle FLEXCUBE Enterprise Limits and Collateral Management, versions 12.3, 12.4, 14.0-14.3, 14.5-14.7
- Oracle FLEXCUBE Universal Banking, versions 12.3, 12.4, 14.0-14.3, 14.5-14.7
- Oracle Fusion Middleware MapViewer, version 12.2.1.4.0
- Oracle Global Lifecycle Management OPatch, versions prior to 12.2.0.1.40
- Oracle GoldenGate Studio, version 12.2.1.4.0
- Oracle GraalVM for JDK, versions 17.0.8, 20.0.2
- Oracle Graph Server and Client, versions 22.4.4 and prior
- Oracle Healthcare Master Person Index, versions 5.0.0-5.0.6
- Oracle HTTP Server, version 12.2.1.4.0
- Oracle Hyperion Infrastructure Technology, version 11.2.14.0.0
- Oracle Identity Manager, version 12.2.1.4.0
- Oracle Java SE, versions 8u381, 8u381-perf, 11.0.20, 17.0.8, 20.0.2
- Oracle Life Sciences InForm, version 7.0.0.0
- Oracle Life Sciences InForm Publisher, version 6.3.1.0
- Oracle Managed File Transfer, version 12.2.1.4.0
- Oracle Middleware Common Libraries and Tools, version 12.2.1.4.0
- Oracle Outside In Technology, version 8.5.6
- Oracle REST Data Services, versions prior to 23.2.2
- Oracle Retail Bulk Data Integration, versions 16.0.3, 19.0.1
- Oracle Retail Customer Management and Segmentation Foundation, versions 18.0.0.13, 19.0.0.7
- Oracle Retail EFTLink, versions 20.0.1, 21.0.0, 22.0.0
- Oracle Retail Financial Integration, versions 14.1.3.2, 15.0.3.1, 16.0.3, 19.0.1
- Oracle Retail Fiscal Management, version 14.2
- Oracle Retail Integration Bus, versions 14.1.3.2, 15.0.3.1, 16.0.3, 19.0.1
- Oracle Retail Merchandising System, version 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 18.0.5, 19.0.4, 20.0.3, 21.0.2, 22.0.0
- Oracle SD-WAN Edge, versions 9.1.1.5.0, 9.1.1.6.0
- Oracle Secure Backup, versions 18.1.0.1.0, 18.1.0.2.0
- Oracle Service Bus, version 12.2.1.4.0
- Oracle SOA Suite, version 12.2.1.4.0
- Oracle Solaris, versions 10, 11
- Oracle Unified Directory, version 12.2.1.4.0
- 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, 4.5.0.0.1, 4.5.0.1.0-4.5.0.1.2
- Oracle Utilities Network Management System, versions 2.3.0.2, 2.4.0.1
- Oracle VM VirtualBox, versions prior to 7.0.12
- Oracle WebCenter Content, version 12.2.1.4.0
- Oracle WebCenter Portal, 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
- PeopleSoft Enterprise CC Common Application Objects, version 9.2
- PeopleSoft Enterprise HCM Global Payroll Switzerland, version 9.2
- PeopleSoft Enterprise PeopleTools, versions 8.59, 8.60
- Primavera Gateway, versions 19.12.0-19.12.17, 20.12.0-20.12.12, 21.12.0-21.12.10

- Primavera Unifier, versions 19.12.0-19.12.16, 20.12.0-20.12.16, 21.12.0-21.12.16, 22.12.0-22.12.9
- Siebel Applications, versions 23.8 and prior
- Sun ZFS Storage Appliance, version 8.8.60
- TimesTen In-Memory Database, versions prior to 18.1.4.38.0, prior to 18.1.4.39.0, prior to 22.1.1.18.0

Identificateurs externes

CVE-2019-10086 CVE-2019-11358 CVE-2019-17498 CVE-2019-20907 CVE-2019-20916
CVE-2020-11022 CVE-2020-11023 CVE-2020-11988 CVE-2020-13956 CVE-2020-1953
CVE-2020-25649 CVE-2020-28493 CVE-2020-29582 CVE-2020-36518 CVE-2020-7760
CVE-2020-9492 CVE-2021-24031 CVE-2021-28165 CVE-2021-33036 CVE-2021-36373
CVE-2021-36374 CVE-2021-37136 CVE-2021-37404 CVE-2021-37533 CVE-2021-37714
CVE-2021-40690 CVE-2021-41164 CVE-2021-41165 CVE-2021-41182 CVE-2021-41183
CVE-2021-41184 CVE-2021-41945 CVE-2021-42575 CVE-2021-43045 CVE-2022-1471
CVE-2022-23491 CVE-2022-23990 CVE-2022-24329 CVE-2022-24407 CVE-2022-24834
CVE-2022-24839 CVE-2022-25147 CVE-2022-25168 CVE-2022-25647 CVE-2022-26612
CVE-2022-27778 CVE-2022-27779 CVE-2022-27780 CVE-2022-27781 CVE-2022-27782
CVE-2022-29546 CVE-2022-29577 CVE-2022-29599 CVE-2022-30115 CVE-2022-31129
CVE-2022-31160 CVE-2022-3171 CVE-2022-33980 CVE-2022-36033 CVE-2022-36944
CVE-2022-37436 CVE-2022-37454 CVE-2022-40151 CVE-2022-40152 CVE-2022-40896
CVE-2022-40897 CVE-2022-40982 CVE-2022-41409 CVE-2022-41704 CVE-2022-41881
CVE-2022-41915 CVE-2022-41954 CVE-2022-41966 CVE-2022-42003 CVE-2022-42004
CVE-2022-4225 CVE-2022-42890 CVE-2022-42898 CVE-2022-42915 CVE-2022-42919
CVE-2022-42920 CVE-2022-43551 CVE-2022-43680 CVE-2022-44729 CVE-2022-44730
CVE-2022-4492 CVE-2022-45061 CVE-2022-45688 CVE-2022-45690 CVE-2022-46908
CVE-2022-48285 CVE-2022-4899 CVE-2023-0361 CVE-2023-0464 CVE-2023-0465
CVE-2023-0466 CVE-2023-0567 CVE-2023-0568 CVE-2023-0662 CVE-2023-1255
CVE-2023-1370 CVE-2023-1436 CVE-2023-2002 CVE-2023-20593 CVE-2023-20860
CVE-2023-20861 CVE-2023-20862 CVE-2023-20863 CVE-2023-20873 CVE-2023-20883
CVE-2023-21829 CVE-2023-22015 CVE-2023-22019 CVE-2023-22025 CVE-2023-22026
CVE-2023-22028 CVE-2023-22029 CVE-2023-22032 CVE-2023-22043 CVE-2023-22059
CVE-2023-22064 CVE-2023-22065 CVE-2023-22066 CVE-2023-22067 CVE-2023-22068
CVE-2023-22069 CVE-2023-22070 CVE-2023-22071 CVE-2023-22072 CVE-2023-22073
CVE-2023-22074 CVE-2023-22075 CVE-2023-22076 CVE-2023-22077 CVE-2023-22078
CVE-2023-22079 CVE-2023-22080 CVE-2023-22081 CVE-2023-22082 CVE-2023-22083
CVE-2023-22084 CVE-2023-22085 CVE-2023-22086 CVE-2023-22087 CVE-2023-22088
CVE-2023-22089 CVE-2023-22090 CVE-2023-22091 CVE-2023-22092 CVE-2023-22093
CVE-2023-22094 CVE-2023-22095 CVE-2023-22096 CVE-2023-22097 CVE-2023-22098
CVE-2023-22099 CVE-2023-22100 CVE-2023-22101 CVE-2023-22102 CVE-2023-22103
CVE-2023-22104 CVE-2023-22105 CVE-2023-22106 CVE-2023-22107 CVE-2023-22108
CVE-2023-22109 CVE-2023-22110 CVE-2023-22111 CVE-2023-22112 CVE-2023-22113
CVE-2023-22114 CVE-2023-22115 CVE-2023-22117 CVE-2023-22118 CVE-2023-22119
CVE-2023-22121 CVE-2023-22122 CVE-2023-22123 CVE-2023-22124 CVE-2023-22125
CVE-2023-22126 CVE-2023-22127 CVE-2023-22128 CVE-2023-22129 CVE-2023-22130
CVE-2023-2283 CVE-2023-22946 CVE-2023-23914 CVE-2023-23915 CVE-2023-23916
CVE-2023-23931 CVE-2023-24998 CVE-2023-25690 CVE-2023-2603 CVE-2023-26048
CVE-2023-26049 CVE-2023-2650 CVE-2023-26604 CVE-2023-27522 CVE-2023-27533
CVE-2023-27534 CVE-2023-28319 CVE-2023-28320 CVE-2023-28321 CVE-2023-28322
CVE-2023-28439 CVE-2023-28484 CVE-2023-28708 CVE-2023-28709 CVE-2023-29402
CVE-2023-29403 CVE-2023-29404 CVE-2023-29405 CVE-2023-29469 CVE-2023-29491

CVE-2023-2975 CVE-2023-2976 CVE-2023-30535 CVE-2023-30585 CVE-2023-30588
CVE-2023-30589 CVE-2023-30590 CVE-2023-30861 CVE-2023-3090 CVE-2023-3247
CVE-2023-33201 CVE-2023-3390 CVE-2023-34034 CVE-2023-34035 CVE-2023-34149
CVE-2023-34396 CVE-2023-3446 CVE-2023-34462 CVE-2023-34981 CVE-2023-35001
CVE-2023-35116 CVE-2023-35788 CVE-2023-35887 CVE-2023-3635 CVE-2023-36479
CVE-2023-36824 CVE-2023-3776 CVE-2023-38039 CVE-2023-3817 CVE-2023-3823
CVE-2023-3824 CVE-2023-38325 CVE-2023-38408 CVE-2023-38545 CVE-2023-38546
CVE-2023-39017 CVE-2023-39022 CVE-2023-4004 CVE-2023-40167 CVE-2023-4039
CVE-2023-41080 CVE-2023-41900 CVE-2023-42503

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

Bulletins de sécurité d’Oracle :

- https://www.oracle.com/security-alerts/cpuoct2023.html