



.....
Centre de Veille de Détection et de
Réaction aux Attaques Informatiques

BULLETIN DE SECURITE

Titre	Mises à jour de sécurité pour plusieurs produits d'oracle
Numéro de Référence	57662210/25
Date de Publication	22 octobre 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Enterprise Manager Base Platform, versions 13.5, 24.1
- GoldenGate Stream Analytics, versions 19.1.0.0.0-19.1.0.0.9
- Identity Manager, versions 12.2.1.4.0, 14.1.2.1.0
- JD Edwards EnterpriseOne Orchestrator, versions 9.2.0.0-9.2.9.4
- JD Edwards EnterpriseOne Tools, versions 9.2.0.0-9.2.9.4
- Management Cloud Engine, version 25.1.0.0.0
- Management Pack for Oracle GoldenGate, version 12.2.1.2.0
- MySQL Cluster, versions 8.0.0-8.0.43, 8.4.0-8.4.6, 9.0.0-9.4.0
- MySQL Enterprise Backup, versions 8.0.0-8.0.42, 8.4.0-8.4.5, 9.0.0-9.3.0
- MySQL Server, versions 8.0.0-8.0.43, 8.4.0-8.4.6, 9.0.0-9.4.0
- MySQL Shell, versions 8.0.40-8.0.43, 8.4.3-8.4.6, 9.1.0-9.4.0
- MySQL Workbench, versions 8.0.0-8.0.43
- Oracle Application Testing Suite, versions 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0
- Oracle Banking Branch, versions 14.5.0.0.0-14.8.0.0.0
- Oracle Banking Corporate Lending Process Management, versions 14.4.0.0.0-14.7.0.0.0
- Oracle Banking Origination, versions 14.5.0.0.0-14.7.0.0.0
- Oracle BI Publisher, versions 7.6.0.0.0, 8.2.0.0.0
- Oracle Business Intelligence Enterprise Edition, versions 7.6.0.0.0, 8.2.0.0.0, 12.2.1.4.0
- Oracle Coherence, versions 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0
- Oracle Commerce Guided Search, version 11.4.0
- Oracle Commerce Platform, version 11.4.0
- Oracle Communications Billing and Revenue Management, versions 12.0.0.4.0-15.0.1.0.0
- Oracle Communications Calendar Server, versions 8.0.0.7.0, 8.0.0.8.0
- Oracle Communications Cloud Native Core Automated Test Suite, versions 24.2.6, 25.1.202
- Oracle Communications Cloud Native Core Binding Support Function, versions 24.2.7-25.1.200
- Oracle Communications Cloud Native Core Certificate Management, version 25.1.200

- Oracle Communications Cloud Native Core Console, versions 24.2.5, 25.1.200
- Oracle Communications Cloud Native Core DBTier, version 25.1.200
- Oracle Communications Cloud Native Core Network Function Cloud Native Environment, versions 25.1.100, 25.1.200
- Oracle Communications Cloud Native Core Network Repository Function, versions 24.2.5, 25.1.202
- Oracle Communications Cloud Native Core Network Slice Selection Function, versions 25.1.100-25.1.200
- Oracle Communications Cloud Native Core Policy, versions 24.2.7-25.1.200
- Oracle Communications Cloud Native Core Security Edge Protection Proxy, versions 24.2.5, 25.1.200, 25.1.201
- Oracle Communications Cloud Native Core Service Communication Proxy, versions 25.1.200, 25.2.100
- Oracle Communications Cloud Native Core Unified Data Repository, versions 25.1.100, 25.1.200
- Oracle Communications Contacts Server, version 8.0.0.9.0
- Oracle Communications Converged Charging System, versions 2.0.0.0.0-2.0.0.1.0
- Oracle Communications Convergence, versions 3.0.3.3.0, 3.0.3.4.0
- Oracle Communications Convergent Charging Controller, versions 12.0.1.0.0-12.0.6.0.0, 15.0.0.0.0-15.0.1.0.0, 15.1.0.0.0
- Oracle Communications Diameter Signaling Router, versions 9.0.0.0.0, 9.1.0.0.0
- Oracle Communications EAGLE Element Management System, versions 46.6, 47.0
- Oracle Communications EAGLE LNP Application Processor, versions 10.2.1.0, 11.0.0.1-11.0.0.2
- Oracle Communications LSMS, versions 13.5.1.0, 14.0.0.1, 14.0.0.2
- Oracle Communications Messaging Server, version 8.1.0.28
- Oracle Communications Network Analytics Data Director, versions 24.2.0-24.2.1, 24.3.0, 25.1.100, 25.1.200
- Oracle Communications Network Charging and Control, versions 12.0.1.0.0-12.0.6.0.0, 15.0.0.0.0-15.0.1.0.0, 15.1.0.0.0
- Oracle Communications Network Integrity, versions 7.3.6, 7.4.0, 7.5.0
- Oracle Communications Offline Mediation Controller, versions 15.0.0.0.0-15.0.1.0.0, 15.1.0.0.0
- Oracle Communications Operations Monitor, versions 5.1, 5.2, 6.0
- Oracle Communications Order and Service Management, versions 7.4.0, 7.4.1, 7.5.0
- Oracle Communications Pricing Design Center, versions 12.0.0.4.0-12.0.0.8.0, 15.0.0.0.0-15.0.1.0.0
- Oracle Communications Service Catalog and Design, versions 8.0.0.5.0, 8.1.0.4.0, 8.2.0.1.0
- Oracle Communications Session Border Controller, versions 4.1.0, 9.0.0, 9.2.0-9.3.0, 10.0.0
- Oracle Communications Unified Assurance, versions 6.1.0-6.1.1
- Oracle Communications Unified Inventory Management, versions 7.5.0-7.5.1, 7.6.0-7.8.0
- Oracle Database Server, versions 19.3-19.28, 21.3-21.19, 23.4-23.9
- Oracle Documaker, versions 12.7.2.4, 13.0.0.3, 13.0.1.1
- Oracle E-Business Suite, versions 12.2.3-12.2.14
- Oracle Enterprise Communications Broker, versions 4.1.0-4.2.0, 5.0.0
- Oracle Enterprise Data Quality, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Enterprise Manager for Fusion Middleware, versions 13.5, 24.1
- Oracle Enterprise Operations Monitor, versions 5.1, 5.2, 6.0
- Oracle Essbase, version 21.7.3.0.0
- Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.7.9, 8.0.8.7, 8.1.2.5
- Oracle Financial Services Behavior Detection Platform, versions 8.0.8.1, 8.1.2.9, 8.1.2.10
- Oracle Financial Services Compliance Studio, version 8.1.2.8
- Oracle Financial Services Model Management and Governance, versions 8.1.2.7, 8.1.3.2
- Oracle Financial Services Revenue Management and Billing, versions 2.9.0.0.0-7.2.0.0.0

- Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition, version 8.0.8
- Oracle Fusion Middleware MapViewer, version 12.2.1.4.0
- Oracle Global Lifecycle Management NextGen OUI Framework, versions 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0
- Oracle GoldenGate, versions 19.1.0.0.0-19.28.0.0.250715, 21.3-21.19, 23.4-23.9
- Oracle GoldenGate Big Data and Application Adapters, versions 21.3-21.19, 23.4-23.9
- Oracle GoldenGate Stream Analytics, versions 19.1.0.0.0-19.1.0.0.12
- Oracle GoldenGate Studio, version 12.2.0.4.0
- Oracle GoldenGate Veridata, versions 12.2.1.4.0-12.2.1.4.250515, 23.1.0.0.0-23.4.0.0.0
- Oracle GraalVM Enterprise Edition, version 21.3.15
- Oracle GraalVM for JDK, versions 17.0.16, 21.0.8
- Oracle Graph Server and Client, versions 24.4.1, 24.4.3, 25.1.0, 25.3.0
- Oracle Health Sciences Data Management Workbench, versions 3.4.0.1.3, 3.4.1.0.10
- Oracle Healthcare Data Repository, version 8.2.0.5
- Oracle Healthcare Master Person Index, versions 5.0.0.0-5.0.9.2
- Oracle Hospitality Cruise Shipboard Property Management (SPMS), version 23.2.5
- Oracle Hyperion Calculation Manager, version 11.2.22.0.0
- Oracle Hyperion Data Relationship Management, version 11.2.22.0.0
- Oracle Hyperion Financial Management, version 11.2.22.0.0
- Oracle Hyperion Infrastructure Technology, version 11.2.22.0.0
- Oracle Hyperion Planning, version 11.2.22.0.0
- Oracle Insurance Policy Administration J2EE, versions 11.3.1-12.0.5
- Oracle Java SE, versions 8u461, 8u461-b50, 8u461-perf, 11.0.28, 17.0.16, 21.0.8, 25
- Oracle JDeveloper, version 12.2.1.4.0
- Oracle Life Sciences InForm, version 7.0.1.0
- Oracle Middleware Common Libraries and Tools, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Outside In Technology, versions 8.5.7, 8.5.8
- Oracle REST Data Services, version 25.2.1
- Oracle Retail Advanced Inventory 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 Invoice Matching, versions 15.0.3.1, 16.0.3
- Oracle Retail Merchandising System, versions 16.0.3, 19.0.1
- Oracle Retail Price Management, versions 15.0.3.1, 16.0.3, 19.0.1
- Oracle Retail Sales Audit, versions 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 Office, versions 20.0.5, 21.0.4, 22.0.2, 23.0.2, 24.0.1, 25.0.0
- Oracle Retail Xstore Point of Service, versions 20.0.5, 21.0.4, 22.0.2, 23.0.2, 24.0.1, 25.0.0
- Oracle Secure Backup, version 19.1.0.1.0
- Oracle Security Service, version 12.2.1.4.0
- Oracle SOA Suite, version 14.1.2.0.0
- Oracle Solaris, version 11
- Oracle Solaris Cluster, version 4
- Oracle Spatial Studio, versions 24.2.0, 25.1.2
- Oracle TimesTen In-Memory Database, versions 18.1.4.1.0-18.1.4.53.0, 22.1.1.1.0-22.1.1.35.0
- Oracle Transportation Management, version 6.5.3
- Oracle Utilities Application Framework, versions 4.3.0.5.0, 4.3.0.6.0, 4.4.0.0.0, 4.4.0.2.0, 4.4.0.3.0, 4.4.0.4.0, 4.5.0.0.0, 4.5.0.1.1, 4.5.0.1.3, 4.5.0.2.0, 24.2.0.0.0, 24.3.0.0.0, 25.4, 25.10
- Oracle Utilities Network Management System, versions 2.4.0.1.31, 2.5.0.1.15, 2.5.0.2.9, 2.6.0.1.8,

2.6.0.2.3

- Oracle VM VirtualBox, versions 7.1.12, 7.2.2
- Oracle WebCenter Forms Recognition, version 14.1.1.0.0
- Oracle WebCenter Portal, version 12.2.1.4.0
- Oracle WebCenter Sites, version 14.1.2.0.0
- Oracle WebLogic Server, versions 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0
- Oracle ZFS Storage Appliance Kit, version 8.8
- PeopleSoft Enterprise CS Financial Aid, version 9.2
- PeopleSoft Enterprise FIN IT Asset Management, version 9.2
- PeopleSoft Enterprise FIN Maintenance Management, version 9.2
- PeopleSoft Enterprise FIN Payables, version 9.2
- PeopleSoft Enterprise PeopleTools, versions 8.60, 8.61, 8.62
- Primavera Gateway, versions 20.12.0-20.12.17, 21.12.0-21.12.15
- Primavera P6 Enterprise Project Portfolio Management, versions 20.12.0.0-20.12.21.0, 21.12.0.0-21.12.21.2, 22.12.0.0-22.12.20.0, 23.12.0.0-23.12.14.0, 24.12.0.0-24.12.4.0
- Primavera Unifier, versions 20.12.0-20.12.16, 21.12.0-21.12.17, 22.12.0-22.12.15, 23.12.0-23.12.15, 24.12.0-24.12.9
- Retail Predictive Application Server, versions 15.0.3, 16.0.3
- Siebel Applications, versions antérieures à 25.10

Identificateurs externes

CVE-2020-11988	CVE-2020-13956	CVE-2020-15250	CVE-2020-17521	CVE-2021-22897
CVE-2021-28165	CVE-2021-3711	CVE-2021-3712	CVE-2022-0839	CVE-2022-22968
CVE-2022-24329	CVE-2022-25647	CVE-2023-1370	CVE-2023-26551	CVE-2023-26552
CVE-2023-26553	CVE-2023-26554	CVE-2023-26555	CVE-2023-2976	CVE-2023-33201
CVE-2023-34053	CVE-2023-34055	CVE-2023-44483	CVE-2023-45853	CVE-2023-5072
CVE-2023-7256	CVE-2024-12133	CVE-2024-12254	CVE-2024-12718	CVE-2024-12797
CVE-2024-12798	CVE-2024-13009	CVE-2024-23807	CVE-2024-26462	CVE-2024-28168
CVE-2024-28182	CVE-2024-35164	CVE-2024-35195	CVE-2024-37370	CVE-2024-37371
CVE-2024-38819	CVE-2024-38820	CVE-2024-38821	CVE-2024-38827	CVE-2024-38828
CVE-2024-4140	CVE-2024-41909	CVE-2024-47554	CVE-2024-48014	CVE-2024-50608
CVE-2024-50609	CVE-2024-51504	CVE-2024-52046	CVE-2024-52533	CVE-2024-52577
CVE-2024-54160	CVE-2024-56406	CVE-2024-57699	CVE-2024-6923	CVE-2024-7254
CVE-2024-8006	CVE-2024-8088	CVE-2024-9143	CVE-2024-9287	CVE-2025-0411
CVE-2025-10148	CVE-2025-1220	CVE-2025-1735	CVE-2025-1795	CVE-2025-1948
CVE-2025-22227	CVE-2025-22228	CVE-2025-22233	CVE-2025-22235	CVE-2025-23084
CVE-2025-23166	CVE-2025-23184	CVE-2025-24189	CVE-2025-24855	CVE-2025-24970
CVE-2025-25193	CVE-2025-25724	CVE-2025-26333	CVE-2025-27113	CVE-2025-27209
CVE-2025-27210	CVE-2025-27363	CVE-2025-27533	CVE-2025-27553	CVE-2025-27587
CVE-2025-27817	CVE-2025-27818	CVE-2025-30474	CVE-2025-30749	CVE-2025-30752
CVE-2025-30754	CVE-2025-30761	CVE-2025-31257	CVE-2025-31273	CVE-2025-31278
CVE-2025-31650	CVE-2025-31651	CVE-2025-31672	CVE-2025-32414	CVE-2025-32415
CVE-2025-32728	CVE-2025-32988	CVE-2025-32989	CVE-2025-32990	CVE-2025-3573
CVE-2025-3576	CVE-2025-41249	CVE-2025-4138	CVE-2025-43211	CVE-2025-43212
CVE-2025-43216	CVE-2025-43227	CVE-2025-43228	CVE-2025-43240	CVE-2025-43265
CVE-2025-4330	CVE-2025-4373	CVE-2025-4435	CVE-2025-4517	CVE-2025-4575
CVE-2025-47273	CVE-2025-4802	CVE-2025-48734	CVE-2025-4877	CVE-2025-4878

CVE-2025-48795	CVE-2025-48924	CVE-2025-48976	CVE-2025-48988	CVE-2025-48989
CVE-2025-49124	CVE-2025-49125	CVE-2025-49128	CVE-2025-4949	CVE-2025-49794
CVE-2025-49795	CVE-2025-49796	CVE-2025-50059	CVE-2025-50063	CVE-2025-50065
CVE-2025-50074	CVE-2025-50075	CVE-2025-50106	CVE-2025-50181	CVE-2025-50182
CVE-2025-5115	CVE-2025-52434	CVE-2025-52520	CVE-2025-52999	CVE-2025-53034
CVE-2025-53035	CVE-2025-53036	CVE-2025-53037	CVE-2025-53040	CVE-2025-53041
CVE-2025-53042	CVE-2025-53043	CVE-2025-53044	CVE-2025-53045	CVE-2025-53046
CVE-2025-53047	CVE-2025-53048	CVE-2025-53049	CVE-2025-53050	CVE-2025-53051
CVE-2025-53052	CVE-2025-53053	CVE-2025-53054	CVE-2025-53055	CVE-2025-53056
CVE-2025-53057	CVE-2025-53058	CVE-2025-53059	CVE-2025-53060	CVE-2025-53061
CVE-2025-53062	CVE-2025-53063	CVE-2025-53064	CVE-2025-53065	CVE-2025-53066
CVE-2025-53067	CVE-2025-53068	CVE-2025-53069	CVE-2025-53070	CVE-2025-53071
CVE-2025-53072	CVE-2025-5318	CVE-2025-53506	CVE-2025-5351	CVE-2025-53547
CVE-2025-53643	CVE-2025-5372	CVE-2025-53816	CVE-2025-53864	CVE-2025-5399
CVE-2025-54090	CVE-2025-5449	CVE-2025-55163	CVE-2025-55212	CVE-2025-55298
CVE-2025-57803	CVE-2025-58057	CVE-2025-5878	CVE-2025-5889	CVE-2025-59375
CVE-2025-59474	CVE-2025-59475	CVE-2025-59476	CVE-2025-5987	CVE-2025-6021
CVE-2025-61748	CVE-2025-61749	CVE-2025-61750	CVE-2025-61751	CVE-2025-61752
CVE-2025-61753	CVE-2025-61754	CVE-2025-61755	CVE-2025-61756	CVE-2025-61757
CVE-2025-61758	CVE-2025-61759	CVE-2025-61760	CVE-2025-61761	CVE-2025-61762
CVE-2025-61763	CVE-2025-61764	CVE-2025-61881	CVE-2025-61882	CVE-2025-61884
CVE-2025-61885	CVE-2025-62287	CVE-2025-62288	CVE-2025-62289	CVE-2025-62290
CVE-2025-62475	CVE-2025-62476	CVE-2025-62477	CVE-2025-62478	CVE-2025-62479
CVE-2025-62480	CVE-2025-62481	CVE-2025-62587	CVE-2025-62588	CVE-2025-62589
CVE-2025-62590	CVE-2025-62591	CVE-2025-62592	CVE-2025-62641	CVE-2025-6395
CVE-2025-6491	CVE-2025-6558	CVE-2025-6965	CVE-2025-7339	CVE-2025-7425
CVE-2025-7962	CVE-2025-8058	CVE-2025-8885	CVE-2025-8916	CVE-2025-9086
CVE-2025-9230	CVE-2025-9232			

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.

L'exploitation de ces vulnérabilités peut permettre à un attaquant distant non authentifié d'exécuter du code arbitraire, d'accéder à des données confidentielles, de contourner des mesures de sécurité 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
- Contournement de mesures de sécurité
- Déni de service

Référence

Bulletin de sécurité d'Oracle :

- <https://www.oracle.com/security-alerts/cpuoct2025.html>