DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 22-01-2025

BULLETIN ALERTES

Object	Multiples vulnérabilités dans plusieurs produits d'Oracle
Réference	1314
Date de Publication	2025-01-22
Sévérité	Critique

IMPACT :

- Exécution de code arbitraire à distance.
- Accès à des informations confidentielles.
- Déni de service

SYSTÉME AFFECTÉ :

- Enterprise Manager for MySQL Database, version 13.5.2.0.0
- JD Edwards EnterpriseOne Orchestrator, versions antérieures à 9.2.9.2
- JD Edwards EnterpriseOne Tools, versions antérieures à 9.2.9.2
- MySQL Cluster, versions 7.6.32 et antérieures, 8.0.40 et antérieures, 8.4.3 et antérieures, 9.1.0 et antérieures
- MySQL Connectors, versions 9.1.0 et antérieures
- MySQL Enterprise Backup, versions 8.0.40 et antérieures, 8.4.3 et antérieures, 9.1.0 et antérieures
- MySQL Enterprise Firewall, versions 8.0.40 et antérieures, 8.4.3 et antérieures, 9.1.0 et antérieures
- MySQL Server, versions 8.0.40 et antérieures, 8.4.3 et antérieures, 9.0.1 et antérieures, 9.1.0 et antérieures
- MySQL Shell, versions 8.0.40 et antérieures, 8.4.3 et antérieures, 9.1.0 et antérieures
- Oracle Agile Engineering Data Management, version 6.2.1
-

Oracle Agile PLM Framework, version 9.3.6

- Oracle Analytics Desktop, versions antérieures à 8.1.0
- Oracle Application Express, versions 23.2, 24.1
- Oracle Application Testing Suite, version 13.3.0.1
- Oracle Banking Corporate Lending Process Management, versions 14.4.0.0.0-14.7.0.0.0
- Oracle Banking Liquidity Management, version 14.7.5.0.0
- Oracle Banking Origination, versions 14.5.0.0.0-14.7.0.0.0
- Oracle BI Publisher, versions 7.0.0.0.0, 7.6.0.0.0
- Oracle Big Data Spatial and Graph, version 3.7
- Oracle Blockchain Platform, versions 21.1.2, 24.1.3
- 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 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 Billing and Revenue Management, versions 12.0.0.4-12.0.0.8, 15.0.0.0-15.0.0.1
- Oracle Communications BRM - Elastic Charging Engine, versions 12.0.0.4-12.0.0.8, 15.0.0.0, 15.0.1.0
- Oracle Communications Cloud Native Core Automated Test Suite, version 24.2.0
- Oracle Communications Cloud Native Core Binding Support Function, versions 24.2.0, 24.2.1
- Oracle Communications Cloud Native Core Certificate Management, version 24.2.1
- Oracle Communications Cloud Native Core Console, version 24.2.1
- Oracle Communications Cloud Native Core DBTier, version 24.3.0
- Oracle Communications Cloud Native Core Network Function Cloud Native Environment, versions 24.2.0, 24.3.0
-

Oracle Communications Cloud Native Core Network Repository Function, version 24.2.2

- Oracle Communications Cloud Native Core Policy, versions 24.2.0-24.2.2
- Oracle Communications Cloud Native Core Security Edge Protection Proxy, versions 23.4.0, 24.2.0, 24.2.1, 24.2.2
- Oracle Communications Cloud Native Core Service Communication Proxy, versions 24.2.0, 24.3.0
- Oracle Communications Cloud Native Core Unified Data Repository, versions 23.4.4, 24.1.1, 24.2.2, 24.2.3, 24.3.0
- Oracle Communications Converged Application Server, versions 8.0, 8.1
- Oracle Communications Convergence, versions 3.0.2.0.0, 3.0.3.0.0, 3.0.3.3.0
- Oracle Communications Diameter Signaling Router, versions 8.2.3.0.0, 8.6.0.4.0, 9.0, 9.0.0.0.0-9.0.2.0.0
- Oracle Communications EAGLE Element Management System, version 47.0.0.0.0
- Oracle Communications Messaging Server, version 8.1.0.26
- Oracle Communications Network Analytics Data Director, versions 24.1.0, 24.2.0

- Oracle Communications Offline Mediation Controller, versions 12.0.0.8, 15.0.0.0, 15.0.1.0
- Oracle Communications Operations Monitor, versions 5.1, 5.2
- Oracle Communications Order and Service Management, versions 7.4.0, 7.4.1, 7.5.0
- Oracle Communications Policy Management, version 15.0.0.0.0
- Oracle Communications Service Catalog and Design, versions 8.0.0.3, 8.1.0.1
- Oracle Communications Session Border Controller, versions 9.2.0, 9.3.0
- Oracle Communications Unified Assurance, versions 6.0.0-6.0.5
- Oracle Communications Unified Inventory Management, versions 7.4.1, 7.4.2, 7.5.1, 7.6.0
- Oracle Communications User Data Repository, versions 12.11, 14.0, 15.0
- Oracle Database Server, versions 19.1, 19.3-19.25, 21.3-21.16, 23.4-23.6
- Oracle Documaker, versions 12.7.1, 12.7.2, 13.0.0
-

Oracle E-Business Suite, versions 12.2.3-12.2.14

- Oracle Enterprise Communications Broker, versions 4.1.0, 4.2.0
- Oracle Enterprise Manager Base Platform, version 13.5.0.0
- Oracle Enterprise Session Border Controller, versions 9.2.0, 9.3.0
- Oracle Essbase, version 21.7
- Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.7.8, 8.0.8.6, 8.1.2.5
- Oracle Financial Services Behavior Detection Platform, versions 8.0.8.1, 8.1.2.7, 8.1.2.8
- Oracle Financial Services Compliance Studio, versions 8.1.2.5, 8.1.2.6
- Oracle Financial Services Enterprise Case Management, versions 8.0.8.2, 8.1.2.7, 8.1.2.8
- Oracle Financial Services Model Management and Governance, versions 8.1.2.6, 8.1.2.7, 8.1.3.0
- Oracle Financial Services Regulatory Reporting, versions 8.1.2.7, 8.1.2.8
- Oracle Financial Services Revenue Management and Billing, versions 2.9.0.0.0-7.0.0.0.0

- 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 GoldenGate, versions 19.1.0.0.0-19.25.0.0.241015, 21.3-21.16, 23.4-23.6
- Oracle GoldenGate Big Data and Application Adapters, versions 19.1.0.0.0-19.1.0.0.18, 21.3.0.0.0-21.16.0.0.0, 23.4-23.6
- Oracle GoldenGate Studio, version 12.2.0.4.0
- Oracle GoldenGate Veridata, versions 12.2.1.4.0-12.2.1.4.240430
- Oracle GraalVM Enterprise Edition, versions 20.3.16, 21.3.12
- Oracle GraalVM for JDK, versions 17.0.13, 21.0.5, 23.0.1
- Oracle Graph Server and Client, versions 23.4.4, 24.4.0
- Oracle Hospitality OPERA 5, versions 5.6.19.20, 5.6.25.8, 5.6.26.6, 5.6.27.1
- Oracle HTTP Server, version 12.2.1.4.0
- Oracle Hyperion Data Relationship Management, version 11.2.19.0.0

- Oracle Identity Manager, version 12.2.1.4.0
- Oracle Java SE, versions 8u431, 8u431-perf, 11.0.25, 17.0.13, 21.0.5, 23.0.1
- Oracle Life Sciences Argus Safety, version 8.2.3
- Oracle Life Sciences Empirica Signal, versions antérieures à 9.2.3
- 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 8.5.7
- Oracle Policy Automation, versions 12.2.18-12.2.36
- Oracle REST Data Services, versions 23.3.0.289.1830, 23.3.1.305.1055, 23.4.0.346.1619, 23.4.1.38.1857, 24.1.0.108.942, 24.1.1.120.1228, 24.1.2.163.1158, 24.2.0, 24.2.0.169.2208, 24.2.1.180.1634, 24.2.2.187.1943, 24.3.0
- Oracle Retail Financial Integration, versions 14.1.3.2, 15.0.3.1, 16.0.3.0, 19.0.1.0
- Oracle Retail Integration Bus, versions 14.1.3.2, 15.0.3.1, 16.0.3.0, 19.0.1.0
-

Oracle SD-WAN Edge, versions 9.1.1.0-9.1.1.9

- Oracle Secure Backup, versions 18.1.0.1.0, 18.1.0.2.0, 19.1.0.0.0
- Oracle Security Service, version 12.2.1.4.0
- Oracle Solaris, version 11
- Oracle TimesTen In-Memory Database, versions 18.1, 22.1
- 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, 4.5.0.1.3, 24.1.0.0.0-24.3.0.0.0
- Oracle Utilities Network Management System, versions 2.5.0.1.14, 2.5.0.1.15, 2.5.0.2.9, 2.6.0.1.5, 2.6.0.1.7
- Oracle Utilities Testing Accelerator, versions 6.0.0.1.0-6.0.0.3.0, 7.0.0.0.0-7.0.0.1.0
- Oracle VM VirtualBox, versions antérieures à 7.0.24, antérieures à 7.1.6
- Oracle WebCenter Portal, version 12.2.1.4.0
- Oracle WebLogic Server, versions 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0
- PeopleSoft Enterprise CC Common Application Objects, version 9.2

- PeopleSoft Enterprise FIN Cash Management, version 9.2
- PeopleSoft Enterprise FIN eSettlements, version 9.2
- PeopleSoft Enterprise PeopleTools, versions 8.60, 8.61
- PeopleSoft Enterprise SCM Purchasing, version 9.2
- Primavera Gateway, versions 20.12.0-20.12.15, 21.12.0-21.12.13
- Primavera P6 Enterprise Project Portfolio Management, versions 20.12.1.0-20.12.21.5, 21.12.1.0-21.12.20.0, 22.12.1.0-22.12.16.0, 23.12.1.0-23.12.10.0
- Primavera Unifier, versions 20.12.0-20.12.16, 21.12.0-21.12.17, 22.12.0-22.12.15, 23.12.0-23.12.12, 24.12.0
- Siebel Applications, versions 24.11 et versions antérieures

DÉSCRIPTION :

Oracle a publié une mise à jour trimestrielle contenant des correctifs de sécurité pour remédier à plusieurs vulnérabilités affectant des dizaines de produits mentionnés dans ce bulletin.Certaines de ces vulnérabilités, jugées critiques, pourraient permettre à un attaquant distant non authentifié d'exécuter du code arbitraire, d'accéder à des données sensibles ou de provoquer un déni de service.

SOLUTION :

Mettre à jour les produits Oracle concernés. (se référer à la documentation)

DOCUMENTATION :

- Bulletin de sécurité d'Oracle:

https://www.oracle.com/security-alerts/cpujan2025.html

- CVE-2023-7272

https://www.cve.org/CVERecord?id=CVE-2023-7272

- CVE-2024-23635

https://www.cve.org/CVERecord?id=CVE-2024-23635

- CVE CVE-2024-29857

https://www.cve.org/CVERecord?id=CVE-2024-29857

- CVE-2024-30171

https://www.cve.org/CVERecord?id=CVE-2024-30171

- CVE-2024-30172

https://www.cve.org/CVERecord?id=CVE-2024-30172

- CVE-2024-34447

https://www.cve.org/CVERecord?id=CVE-2024-34447

- CVE-2024-47554

https://www.cve.org/CVERecord?id=CVE-2024-47554

- CVE-2025-21535

https://www.cve.org/CVERecord?id=CVE-2025-21535

- CVE-2025-21549

https://www.cve.org/CVERecord?id=CVE-2025-21549

- CVE-2025-21533

https://www.cve.org/CVERecord?id=CVE-2025-21533

- CVE-2025-21571

https://www.cve.org/CVERecord?id=CVE-2025-21571

- CVE-2025-21551

https://www.cve.org/CVERecord?id=CVE-2025-21551

- CVE-2020-22218

https://www.cve.org/CVERecord?id=CVE-2020-22218

- CVE-2023-48795

https://www.cve.org/CVERecord?id=CVE-2023-48795

- CVE-2024-0397

https://www.cve.org/CVERecord?id=CVE-2024-0397

- CVE-2024-22018

https://www.cve.org/CVERecord?id=CVE-2024-22018

- CVE-2024-22019

https://www.cve.org/CVERecord?id=CVE-2024-22019

- CVE-2024-22020

https://www.cve.org/CVERecord?id=CVE-2024-22020

- CVE-2024-2511

https://www.cve.org/CVERecord?id=CVE-2024-2511

- CVE-2024-27280

https://www.cve.org/CVERecord?id=CVE-2024-27280

- CVE-2024-27281

https://www.cve.org/CVERecord?id=CVE-2024-27281

- CVE-2024-27282

https://www.cve.org/CVERecord?id=CVE-2024-27282

- CVE-2024-28849

https://www.cve.org/CVERecord?id=CVE-2024-28849

- CVE-2024-29025

https://www.cve.org/CVERecord?id=CVE-2024-29025

- CVE-2024-35195

https://www.cve.org/CVERecord?id=CVE-2024-35195

- CVE-2024-36137

https://www.cve.org/CVERecord?id=CVE-2024-36137

- CVE-2024-36138

https://www.cve.org/CVERecord?id=CVE-2024-36138

- CVE-2024-37372

https://www.cve.org/CVERecord?id=CVE-2024-37372

- CVE-2024-37891

https://www.cve.org/CVERecord?id=CVE-2024-37891

- CVE-2024-4030

https://www.cve.org/CVERecord?id=CVE-2024-4030

- CVE-2024-4032

https://www.cve.org/CVERecord?id=CVE-2024-4032

- CVE-2024-4603

https://www.cve.org/CVERecord?id=CVE-2024-4603

- CVE-2024-4741

https://www.cve.org/CVERecord?id=CVE-2024-4741

- CVE-2024-5535

https://www.cve.org/CVERecord?id=CVE-2024-5535

- CVE-2024-6119

https://www.cve.org/CVERecord?id=CVE-2024-6119

- CVE-2024-6232

https://www.cve.org/CVERecord?id=CVE-2024-6232

- CVE-2024-7592

https://www.cve.org/CVERecord?id=CVE-2024-7592

- CVE-2025-21530

https://www.cve.org/CVERecord?id=CVE-2025-21530

- CVE-2025-21537

https://www.cve.org/CVERecord?id=CVE-2025-21537

- CVE-2025-21539

https://www.cve.org/CVERecord?id=CVE-2025-21539

- CVE-2025-21545

https://www.cve.org/CVERecord?id=CVE-2025-21545

- CVE-2025-21561

https://www.cve.org/CVERecord?id=CVE-2025-21561

- CVE-2025-21562

https://www.cve.org/CVERecord?id=CVE-2025-21562

- CVE-2025-21563

https://www.cve.org/CVERecord?id=CVE-2025-21563

- CVE-2024-11053

https://www.cve.org/CVERecord?id=CVE-2024-11053

- CVE-2024-37370

https://www.cve.org/CVERecord?id=CVE-2024-37370

- CVE-2024-37371

https://www.cve.org/CVERecord?id=CVE-2024-37371

- CVE-2024-38819

https://www.cve.org/CVERecord?id=CVE-2024-38819

- CVE-2024-38820

https://www.cve.org/CVERecord?id=CVE-2024-38820

- CVE-2025-21490

https://www.cve.org/CVERecord?id=CVE-2025-21490

- CVE-2025-21491

https://www.cve.org/CVERecord?id=CVE-2025-21491

- CVE-2025-21492

https://www.cve.org/CVERecord?id=CVE-2025-21492

- CVE-2025-21493

https://www.cve.org/CVERecord?id=CVE-2025-21493

- CVE-2025-21494

https://www.cve.org/CVERecord?id=CVE-2025-21494

- CVE-2025-21495

https://www.cve.org/CVERecord?id=CVE-2025-21495

- CVE-2025-21497

https://www.cve.org/CVERecord?id=CVE-2025-21497

- CVE-2025-21499

https://www.cve.org/CVERecord?id=CVE-2025-21499

- CVE-2025-21500

https://www.cve.org/CVERecord?id=CVE-2025-21500

- CVE-2025-21501

https://www.cve.org/CVERecord?id=CVE-2025-21501

- CVE-2025-21503

https://www.cve.org/CVERecord?id=CVE-2025-21503

- CVE-2025-21504

https://www.cve.org/CVERecord?id=CVE-2025-21504

- CVE-2025-21505

https://www.cve.org/CVERecord?id=CVE-2025-21505

- CVE-2025-21518

https://www.cve.org/CVERecord?id=CVE-2025-21518

- CVE-2025-21519

https://www.cve.org/CVERecord?id=CVE-2025-21519

- CVE-2025-21520

https://www.cve.org/CVERecord?id=CVE-2025-21520

- CVE-2025-21521

https://www.cve.org/CVERecord?id=CVE-2025-21521

- CVE-2025-21522

https://www.cve.org/CVERecord?id=CVE-2025-21522

- CVE-2025-21523

https://www.cve.org/CVERecord?id=CVE-2025-21523

- CVE-2025-21525

https://www.cve.org/CVERecord?id=CVE-2025-21525

- CVE-2025-21529

https://www.cve.org/CVERecord?id=CVE-2025-21529

- CVE-2025-21531

https://www.cve.org/CVERecord?id=CVE-2025-21531

- CVE-2025-21534

https://www.cve.org/CVERecord?id=CVE-2025-21534

- CVE-2025-21536

https://www.cve.org/CVERecord?id=CVE-2025-21536

- CVE-2025-21540

https://www.cve.org/CVERecord?id=CVE-2025-21540

- CVE-2025-21543

https://www.cve.org/CVERecord?id=CVE-2025-21543

- CVE-2025-21546

https://www.cve.org/CVERecord?id=CVE-2025-21546

- CVE-2025-21548

https://www.cve.org/CVERecord?id=CVE-2025-21548

- CVE-2025-21555

https://www.cve.org/CVERecord?id=CVE-2025-21555

- CVE-2025-21559

https://www.cve.org/CVERecord?id=CVE-2025-21559

- CVE-2025-21566

https://www.cve.org/CVERecord?id=CVE-2025-21566

- CVE-2025-21567

https://www.cve.org/CVERecord?id=CVE-2025-21567

- CVE-2025-0509

https://www.cve.org/CVERecord?id=CVE-2025-0509

- CVE-2025-21502

https://www.cve.org/CVERecord?id=CVE-2025-21502

- CVE CVE-2022-26345

https://www.cve.org/CVERecord?id=CVE-2022-26345

- CVE-2023-48795

https://www.cve.org/CVERecord?id=CVE-2023-48795

- CVE-2023-52428

https://www.cve.org/CVERecord?id=CVE-2023-52428

- CVE-2024-21211

https://www.cve.org/CVERecord?id=CVE-2024-21211

- CVE-2025-21553

https://www.cve.org/CVERecord?id=CVE-2025-21553

- CVE-2016-1000027

https://nvd.nist.gov/vuln/detail/CVE-2016-1000027

- CVE-2019-11065

https://nvd.nist.gov/vuln/detail/CVE-2019-11065

- CVE-2019-12415

https://nvd.nist.gov/vuln/detail/CVE-2019-12415

- CVE-2019-15052

https://nvd.nist.gov/vuln/detail/CVE-2019-15052

- CVE-2019-16370

https://nvd.nist.gov/vuln/detail/CVE-2019-16370

- CVE-2020-11979

https://nvd.nist.gov/vuln/detail/CVE-2020-11979

- CVE-2020-13956

https://nvd.nist.gov/vuln/detail/CVE-2020-13956

- CVE-2020-22218

https://nvd.nist.gov/vuln/detail/CVE-2020-22218