



BULLETIN DE SECURITE

Titre	"Oracle Critical Patch Update" du Mois Avril 2025
Numéro de Référence	54021704/25
Date de Publication	17 Avril 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Autonomous Health Framework, versions 23.8.0-23.11.0, 24.1.0-24.11.0, 25.1.0, 25.2.0
- GoldenGate Stream Analytics, versions 19.1.0.0.0-19.1.0.0.10
- JD Edwards EnterpriseOne Tools, versions 9.2.0.0-9.2.9.2
- Management Cloud Engine, version 24.3.0
- MySQL Client, versions 8.0.0-8.0.41, 8.4.0-8.4.4, 9.0.0-9.2.0
- MySQL Cluster, versions 7.6.0-7.6.33, 8.0.0-8.0.41, 8.4.0-8.4.4, 9.0.0-9.2.0
- MySQL Connectors, versions 9.0.0-9.2.0
- MySQL Enterprise Backup, versions 8.0.0-8.0.41, 8.4.0-8.4.4, 9.0.0-9.2.0
- MySQL Server, versions 8.0.0-8.0.41, 8.4.0-8.4.4, 9.0.0-9.2.0
- MySQL Shell, versions 8.0.32-8.0.41, 8.4.0-8.4.4, 9.0.0-9.2.0
- MySQL Workbench, versions 8.0.0-8.0.41
- Oracle Access Manager, version 12.2.1.4.0
- Oracle Agile Engineering Data Management, version 6.2.1
- Oracle Application Express, versions 23.2.15, 23.2.16, 24.1.9, 24.1.10, 24.2.3, 24.2.4
- Oracle Application Testing Suite, version 13.3.0.1
- Oracle Banking APIs, versions 21.1.0.0.0, 22.1.0.0.0, 22.2.0.0.0
- Oracle Banking Corporate Lending Process Management, versions 14.5.0.0.0-14.7.0.0.0
- Oracle Banking Digital Experience, versions 21.1.0.0.0, 22.1.0.0.0, 22.2.0.0.0
- Oracle Banking Liquidity Management, version 14.7.0.7.0
- Oracle Banking Origination, versions 14.5.0.0.0-14.7.0.0.0

- Oracle BI Publisher, versions 7.6.0.0.0, 12.2.1.4.0
- Oracle Business Activity Monitoring, version 14.1.2.0.0
- Oracle Business Intelligence Enterprise Edition, versions 7.6.0.0.0, 12.2.1.4.0
- Oracle Business Process Management Suite, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Coherence, versions 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0
- Oracle Commerce Guided Search, versions 11.3.2, 11.4.0
- Oracle Commerce Merchandising, versions 11.3.0, 11.3.1, 11.3.2
- Oracle Commerce Platform, versions 11.3.0, 11.3.1, 11.3.2, 11.4.0
- Oracle Communications Billing and Revenue Management, versions 12.0.0.4.0-12.0.0.8.0, 15.0.0.0.0-15.0.1.0.0
- Oracle Communications Cloud Native Core Binding Support Function, versions 24.2.0-24.2.2
- Oracle Communications Cloud Native Core Certificate Management, version 24.2.2
- Oracle Communications Cloud Native Core Console, version 24.2.2
- Oracle Communications Cloud Native Core DBTier, versions 24.2.3, 24.2.4, 24.3.0
- Oracle Communications Cloud Native Core Network Data Analytics Function, version 24.2.0
- Oracle Communications Cloud Native Core Network Function Cloud Native Environment, versions 24.2.5, 25.1.100
- Oracle Communications Cloud Native Core Network Repository Function, version 24.2.3
- Oracle Communications Cloud Native Core Policy, versions 24.2.0-24.2.4
- Oracle Communications Cloud Native Core Security Edge Protection Proxy, versions 24.2.2, 24.2.3, 24.3.0
- Oracle Communications Cloud Native Core Service Communication Proxy, versions 24.2.0, 24.2.3, 24.3.0, 25.1.100
- Oracle Communications Cloud Native Core Unified Data Repository, versions 22.4.0, 23.1.0-23.4.0, 24.2.3, 25.1.100
- Oracle Communications Diameter Signaling Router, version 9.0.0.0
- Oracle Communications EAGLE Element Management System, version 46.6
- Oracle Communications Element Manager, versions 9.0.0-9.0.3
- Oracle Communications Messaging Server, version 8.1.0.26.0
- Oracle Communications MetaSolv Solution, version 6.3.1
- Oracle Communications Network Analytics Data Director, versions 24.1.0-24.3.0
- Oracle Communications Network Charging and Control, versions 12.0.6.0.0, 15.0.0.0.0, 15.0.1.0.0

- Oracle Communications Network Integrity, versions 7.3.6, 7.4.0, 7.5.0
- Oracle Communications Operations Monitor, version 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 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 8.0.0.4.0, 8.1.0.2.0
- Oracle Communications Session Border Controller, versions 9.2.0, 9.3.0, 10.0.0
- Oracle Communications Session Report Manager, versions 9.0.0-9.0.3
- Oracle Communications Unified Assurance, versions 6.0-6.1
- Oracle Communications Unified Inventory Management, versions 7.4.0-7.4.2, 7.5.0-7.5.1, 7.6.0, 7.7.0
- Oracle Communications User Data Repository, versions 14.0.0, 15.0.0, 15.0.1, 15.0.2
- Oracle Data Integrator, version 12.2.1.4.0
- Oracle Database Server, versions 19.3-19.26, 21.3-21.17, 23.4-23.7
- Oracle Demantra Demand Management, versions 12.2.6-12.2.14
- Oracle Documaker, versions 12.7.1.6, 12.7.2.3, 13.0.0.1
- Oracle E-Business Suite, versions 12.2.3-12.2.14, [ECC] 12-13
- Oracle Enterprise Communications Broker, versions 4.1.0, 4.2.0
- Oracle Enterprise Manager Base Platform, versions 13.5.0.0.0, 24.1.0.0.0
- Oracle Essbase, version 21.7.1.0.0
- Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.7.8, 8.0.8.6, 8.1.1.4, 8.1.2.5
- Oracle Financial Services Behavior Detection Platform, versions 8.0.8.1, 8.1.2.8, 8.1.2.9
- Oracle Financial Services Compliance Studio, version 8.1.2.9
- Oracle Financial Services Model Management and Governance, version 8.1.2.7.0
- 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 19.1.0.0.0-19.26.0.0.250219, 21.3-21.17, 23.4-23.7
- Oracle GoldenGate Veridata, versions 12.2.1.4.0-12.2.1.4.241210
- Oracle GraalVM Enterprise Edition, versions 20.3.17, 21.3.13
- Oracle GraalVM for JDK, versions 17.0.14, 21.0.6, 24

- Oracle Graph Server and Client, versions 23.4.3, 23.4.4, 24.3.0, 24.4.0
- Oracle Hospitality Cruise Shipboard Property Management System, version 23.2.1
- Oracle Hospitality Reporting and Analytics, versions 9.1.34-9.1.36
- Oracle Hospitality Symphony, versions 19.1-19.7
- Oracle HTTP Server, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Hyperion Financial Reporting, version 11.2.19.0.0
- Oracle Hyperion Infrastructure Technology, version 11.2.19.0.0
- Oracle Java SE, versions 8u441, 8u441-perf, 11.0.26, 17.0.14, 21.0.6, 24
- Oracle JDeveloper, version 12.2.1.4.0
- Oracle Managed File Transfer, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle NoSQL Database, versions 1.5.0, 1.6.0, 1.6.1
- Oracle Outside In Technology, version 8.5.7
- Oracle Policy Automation, versions 12.2.0-12.2.36
- Oracle Policy Modeling, versions 12.2.0-12.2.36
- Oracle REST Data Services, versions 23.1, 23.2, 23.3, 23.4
- Oracle Retail Order Broker, version 19.1
- Oracle Retail Store Inventory Management, version 16.0.3.16
- Oracle Retail Xstore Point of Service, versions 19.0.6, 20.0.5, 21.0.4, 22.0.2, 23.0.2, 24.0.1
- Oracle SD-WAN Aware, version 9.0.1.11
- Oracle SD-WAN Edge, version 9.1.1.9
- Oracle Secure Backup, versions 12.1.0.1, 12.1.0.2, 12.1.0.3, 18.1.0.0, 18.1.0.1, 18.1.0.2, 19.1.0.0
- Oracle Service Bus, version 12.2.1.4.0
- Oracle Smart View for Office, version 24.200
- Oracle SOA Suite, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Solaris, version 11
- Oracle SQL Developer, version 24.3.1.347.1826
- Oracle TimesTen In-Memory Database, versions 22.1.1.1.0-22.1.1.30.0
- 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 VM VirtualBox, version 7.1.6
- Oracle WebCenter Forms Recognition, version 14.1.1.0.0
- Oracle WebCenter Portal, version 12.2.1.4.0

- Oracle WebLogic Server, versions 12.2.1.4.0, 14.1.1.0.0
- OSS Support Tools, versions 2.11.0-2.12.46, 8.0-8.18, 18.1-18.4, 19.1-19.4, 20.1-20.4, 22.2, 23.1-23.4, 24.1-24.4, 25.1
- PeopleSoft Enterprise CC Common Application Objects, version 9.2
- PeopleSoft Enterprise HCM Talent Acquisition Manager, 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 22.12.0-22.12.18, 23.12.0-23.12.13, 24.12.0-24.12.2
- Primavera Unifier, versions 20.12.0-20.12.16, 21.12.0-21.12.17, 22.12.0-22.12.15, 23.12.0-23.12.13, 24.12.0-24.12.3
- Siebel Applications, versions 17.0-25.2

Identificateurs externes

- CVE-2016-1000027 CVE-2020-11996 CVE-2020-13935
- CVE-2020-13936 CVE-2020-13943 CVE-2020-1935
- CVE-2020-1938 CVE-2020-25649 CVE-2020-36518
- CVE-2020-36843 CVE-2020-9484 CVE-2021-23450
- CVE-2021-24122 CVE-2021-25122 CVE-2021-25329
- CVE-2021-28170 CVE-2021-30640 CVE-2021-31684
- CVE-2021-33037 CVE-2021-37714 CVE-2021-41079
- CVE-2021-41184 CVE-2021-41973 CVE-2021-42575
- CVE-2021-43980 CVE-2021-46877 CVE-2022-25762
- CVE-2022-34169 CVE-2022-34381 CVE-2022-36033
- CVE-2022-3786 CVE-2022-42003 CVE-2022-42004
- CVE-2022-42252 CVE-2022-45047 CVE-2023-1370
- CVE-2023-24998 CVE-2023-25399 CVE-2023-26464
- CVE-2023-28708 CVE-2023-34053 CVE-2023-35116
- CVE-2023-35887 CVE-2023-36479 CVE-2023-37536
- CVE-2023-38546 CVE-2023-39410 CVE-2023-40167
- CVE-2023-40743 CVE-2023-41080 CVE-2023-42795
- CVE-2023-44487 CVE-2023-45648 CVE-2023-46589
- CVE-2023-48795 CVE-2023-49582 CVE-2023-51074
- CVE-2023-51441 CVE-2023-52428 CVE-2023-5388
- CVE-2023-5685 CVE-2024-11053 CVE-2024-11233

- CVE-2024-11234 CVE-2024-11236 CVE-2024-1135
- CVE-2024-11612 CVE-2024-12797 CVE-2024-12798
- CVE-2024-12801 CVE-2024-13176 CVE-2024-21538
- CVE-2024-22243 CVE-2024-23672 CVE-2024-23807
- CVE-2024-24549 CVE-2024-25638 CVE-2024-25710
- CVE-2024-26308 CVE-2024-27856 CVE-2024-28168
- CVE-2024-28219 CVE-2024-28834 CVE-2024-28835
- CVE-2024-29025 CVE-2024-29131 CVE-2024-29133
- CVE-2024-29736 CVE-2024-29857 CVE-2024-30172
- CVE-2024-31141 CVE-2024-32007 CVE-2024-34064
- CVE-2024-35195 CVE-2024-36114 CVE-2024-37891
- CVE-2024-38357 CVE-2024-38474 CVE-2024-38476
- CVE-2024-38816 CVE-2024-38819 CVE-2024-38820
- CVE-2024-38827 CVE-2024-38828 CVE-2024-38998
- CVE-2024-38999 CVE-2024-39338 CVE-2024-39573
- CVE-2024-39884 CVE-2024-40725 CVE-2024-40866
- CVE-2024-40896 CVE-2024-4227 CVE-2024-42367
- CVE-2024-43044 CVE-2024-43045 CVE-2024-43709
- CVE-2024-43796 CVE-2024-44185 CVE-2024-44187
- CVE-2024-44244 CVE-2024-44296 CVE-2024-44308
- CVE-2024-44309 CVE-2024-45337 CVE-2024-45338
- CVE-2024-45613 CVE-2024-47072 CVE-2024-47197
- CVE-2024-47535 CVE-2024-47544 CVE-2024-47545
- CVE-2024-47546 CVE-2024-47554 CVE-2024-47561
- CVE-2024-47596 CVE-2024-47597 CVE-2024-47606
- CVE-2024-47775 CVE-2024-47776 CVE-2024-47777
- CVE-2024-47778 CVE-2024-49767 CVE-2024-49771
- CVE-2024-50379 CVE-2024-50602 CVE-2024-52046
- CVE-2024-5206 CVE-2024-52303 CVE-2024-52316
- CVE-2024-52317 CVE-2024-53122 CVE-2024-53382
- CVE-2024-54479 CVE-2024-54502 CVE-2024-54505
- CVE-2024-54508 CVE-2024-54534 CVE-2024-54543
- CVE-2024-54677 CVE-2024-5535 CVE-2024-56128

- CVE-2024-56171 CVE-2024-56201 CVE-2024-56326
- CVE-2024-56337 CVE-2024-57699 CVE-2024-6119
- CVE-2024-6763 CVE-2024-7254 CVE-2024-7264
- CVE-2024-8176 CVE-2024-8184 CVE-2024-8775
- CVE-2024-9143 CVE-2024-9681 CVE-2024-9902
- CVE-2025-1974 CVE-2025-21502 CVE-2025-21573
- CVE-2025-21574 CVE-2025-21575 CVE-2025-21576
- CVE-2025-21577 CVE-2025-21578 CVE-2025-21579
- CVE-2025-21580 CVE-2025-21581 CVE-2025-21582
- CVE-2025-21583 CVE-2025-21584 CVE-2025-21585
- CVE-2025-21586 CVE-2025-21587 CVE-2025-21588
- CVE-2025-22228 CVE-2025-23022 CVE-2025-23083
- CVE-2025-23084 CVE-2025-23085 CVE-2025-23184
- CVE-2025-24143 CVE-2025-24150 CVE-2025-24158
- CVE-2025-24162 CVE-2025-24813 CVE-2025-24928
- CVE-2025-24970 CVE-2025-25193 CVE-2025-26465
- CVE-2025-26466 CVE-2025-26791 CVE-2025-27113
- CVE-2025-27363 CVE-2025-27516 CVE-2025-27789
- CVE-2025-30681 CVE-2025-30682 CVE-2025-30683
- CVE-2025-30684 CVE-2025-30685 CVE-2025-30686
- CVE-2025-30687 CVE-2025-30688 CVE-2025-30689
- CVE-2025-30690 CVE-2025-30691 CVE-2025-30692
- CVE-2025-30693 CVE-2025-30694 CVE-2025-30695
- CVE-2025-30696 CVE-2025-30697 CVE-2025-30698
- CVE-2025-30699 CVE-2025-30700 CVE-2025-30701
- CVE-2025-30702 CVE-2025-30703 CVE-2025-30704
- CVE-2025-30705 CVE-2025-30706 CVE-2025-30707
- CVE-2025-30708 CVE-2025-30709 CVE-2025-30710
- CVE-2025-30711 CVE-2025-30712 CVE-2025-30713
- CVE-2025-30714 CVE-2025-30715 CVE-2025-30716
- CVE-2025-30717 CVE-2025-30718 CVE-2025-30719
- CVE-2025-30720 CVE-2025-30721 CVE-2025-30722
- CVE-2025-30723 CVE-2025-30724 CVE-2025-30725

- CVE-2025-30726 CVE-2025-30727 CVE-2025-30728
- CVE-2025-30729 CVE-2025-30730 CVE-2025-30731
- CVE-2025-30732 CVE-2025-30733 CVE-2025-30735
- CVE-2025-30736 CVE-2025-30737 CVE-2025-30740
- CVE-2025-31720 CVE-2025-31721

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 Avril 2025. 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 Avril 2025, 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 Avril 2025:

- <https://www.oracle.com/security-alerts/cpuapr2025.html>