ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	"Oracle Critical Patch Update" du Mois Avril 2026
Numéro de Référence	63432204/26
Date de Publication	22 Avril 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- JD Edwards EnterpriseOne Tools, versions 9.2.0.0-9.2.26.1
- Management Cloud Engine, version 25.2.0.0.0
- MySQL Cluster, versions 8.0.0-8.0.44, 8.4.0-8.4.7, 9.0.0-9.5.0
- MySQL Connectors, versions 9.0.0-9.6.0
- MySQL Enterprise Backup, versions 8.0.0-8.0.45, 8.4.0-8.4.8, 9.0.0-9.6.0
- MySQL Server, versions 8.0.0-8.0.45, 8.4.0-8.4.8, 9.0.0-9.6.0
- MySQL Shell, versions 8.0.0-8.0.45, 8.4.0-8.4.8, 9.0.0-9.6.0
- MySQL Workbench, versions 8.0.0-8.0.46
- Oracle Access Manager, version 14.1.2.0.0
- Oracle Adapter for Eclipse RDF4J, versions 3.12.0, 21.1.8, 24.1.0
- Oracle Agile Product Lifecycle Management for Process, version 6.2.4
- Oracle Application Development Framework (ADF), versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Application Express, versions 23.2.20, 23.2.21, 24.1.15, 24.1.16, 24.2.13, 24.2.15
- Oracle Application Testing Suite, version 13.3.0.1
- Oracle Autonomous Health Framework, versions 25.11-26.1
- Oracle AutoVue, version 21.1.0
- Oracle Banking Branch, versions 14.5.0.0.0-14.8.0.0.0
- Oracle Banking Cash Management, version 14.8.2.0.0
- Oracle Banking Collections and Recovery, versions 14.6.0.0.0-14.8.0.0.0
- Oracle Banking Corporate Lending, versions 14.5.0.0.0-14.8.0.0.0

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – 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 ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- Oracle Banking Corporate Lending Process Management, versions 14.5.0.0.0-14.8.0.0.0
- Oracle Banking Credit Facilities Process Management, versions 14.5.0.0.0-14.8.0.0.0
- Oracle Banking Liquidity Management, versions 14.8.0.0.0, 14.8.1.0.0
- Oracle Banking Origination, versions 14.5.0.0.0-14.8.0.0.0
- Oracle Banking Payments, versions 14.5.0.0.0-14.8.0.0.0
- Oracle Banking Supply Chain Finance, versions 14.5.0.0.0-14.8.0.0.0
- Oracle Banking Trade Finance, versions 14.5.0.0.0-14.8.0.0.0
- Oracle Banking Trade Finance Process Management, versions 14.5.0.0.0-14.8.0.0.0
- Oracle Banking Virtual Account Management, versions 14.5.0.0.0-14.8.0.0.0
- Oracle BI Publisher, versions 7.6.0.0.0, 8.2.0.0.0
- Oracle Blockchain Platform, version 24.1.3
- Oracle Business Activity Monitoring, version 12.2.1.4.0
- Oracle Business Intelligence Enterprise Edition, versions 7.6.0.0.0, 8.2.0.0.0
- Oracle Business Process Management Suite, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Commerce Guided Search, version 11.4.0
- Oracle Communications Billing and Revenue Management, versions 15.0.0.0.0-15.0.1.0.0, 15.1.0.0.0-15.2.0.0.0
- Oracle Communications BRM - Elastic Charging Engine, versions 15.0.0.0-15.0.1.0, 15.1.0.0-15.2.0.0
- Oracle Communications Cloud Native Core Binding Support Function, version 25.1.200
- Oracle Communications Cloud Native Core Certificate Management, version 25.1.201
- Oracle Communications Cloud Native Core Console, version 25.1.201
- Oracle Communications Cloud Native Core DBTier, versions 25.1.200, 25.2.100
- Oracle Communications Cloud Native Core Network Exposure Function, versions 24.2.1, 24.2.4
- Oracle Communications Cloud Native Core Network Function Cloud Native Environment, versions 25.1.200, 25.2.200
- Oracle Communications Cloud Native Core Network Repository Function, version 25.1.204
- Oracle Communications Cloud Native Core Network Slice Selection Function, versions 25.1.100, 25.1.200
- Oracle Communications Cloud Native Core Policy, versions 25.1.200, 25.1.201, 25.1.202
- Oracle Communications Cloud Native Core Security Edge Protection Proxy, versions 25.1.200, 25.1.201, 25.2.100

- Oracle Communications Cloud Native Core Service Communication Proxy, versions 25.1.100, 25.1.200, 25.1.202, 25.2.100
- Oracle Communications Cloud Native Core Unified Data Repository, versions 25.1.100, 25.1.200
- Oracle Communications Convergence, version 3.0.3.4.0
- Oracle Communications EAGLE, version 47.0
- Oracle Communications EAGLE Application Processor, versions 17.0-17.1
- Oracle Communications EAGLE Element Management System, version 47.0.0.1.0
- Oracle Communications EAGLE LNP Application Processor, version 11.0
- Oracle Communications Element Manager, versions 9.0.0-9.0.4
- Oracle Communications Instant Messaging Server, version 10.0.1.8.0
- Oracle Communications LSMS, version 14.0
- Oracle Communications Messaging Server, version 8.1.0.0.0
- Oracle Communications Network Integrity, versions 7.3.6, 7.4.0, 7.5.0, 8.0.0
- Oracle Communications Offline Mediation Controller, versions 15.0.0.0.0-15.0.1.0.0, 15.1.0.0.0-15.2.0.0.0
- Oracle Communications Operations Monitor, versions 5.2, 6.0, 6.1
- Oracle Communications Order and Service Management, versions 7.5.0, 8.0.0
- Oracle Communications Performance Intelligence Center, versions 10.5.0.0-10.5.0.2
- Oracle Communications Policy Management, versions 15.0.0.0.0, 15.0.0.1.0
- Oracle Communications Service Catalog and Design, versions 8.0.0.6.0, 8.1.0.5.0, 8.2.0.2.0
- Oracle Communications Session Border Controller, versions 9.3.0, 10.0.0, 10.1.0
- Oracle Communications Session Report Manager, versions 9.0.0-9.0.4
- Oracle Communications Unified Assurance, versions 6.1.1-7.0.0
- Oracle Communications Unified Inventory Management, versions 7.5.0-7.5.1, 7.6.0-7.8.0, 8.0.0
- Oracle Configuration Manager, versions 13.5, 24.1
- Oracle Data Integrator, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Database Server, versions 12.1.0.2.0, 12.2.0.1.0, 19.3-19.30, 21.3-21.21, 23.4.0-23.26.1
- Oracle Documaker, versions 12.7.2-13.0.2
- Oracle E-Business Suite, versions 12.2.3-12.2.15, 15.0
- Oracle Enterprise Communications Broker, versions 4.2.0, 5.0.0
- Oracle Enterprise Manager Base Platform, versions 13.5, 24.1

- Oracle Enterprise Manager for Fusion Middleware, versions 13.5, 24.1
- Oracle Enterprise Operations Monitor, version 6.1.0.0.0
- Oracle Essbase, version 21.8.1.0.0
- 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, 8.1.2.10, 8.1.2.11
- Oracle Financial Services Compliance Studio, version 8.1.2.9
- Oracle Financial Services Customer Screening, version 8.1.2.8.0
- Oracle Financial Services Enterprise Case Management, versions 8.0.8.2, 8.1.2.10, 8.1.2.11
- Oracle Financial Services Lending and Leasing, versions 14.8.0.0.0, 14.10.0.0.0-14.12.0.0.0
- Oracle Financial Services Model Management and Governance, version 8.1.2.7
- Oracle Financial Services Regulatory Reporting, versions 8.1.2.10, 8.1.2.11
- Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition, version 8.0.8
- Oracle Financial Services Transaction Filtering, version 8.1.2.8.0
- Oracle FLEXCUBE Enterprise Limits and Collateral Management, versions 14.5.0.0.0-14.8.0.0.0
- Oracle Fusion Middleware, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Global Lifecycle Management OPatchAuto, versions 12.2.0.1.16-12.2.0.1.49
- Oracle GoldenGate, versions 23.4-23.26.1
- Oracle GoldenGate Big Data and Application Adapters, versions 19.1.0.0.0-19.1.0.0.21, 21.3-21.21, 23.4-23.10
- Oracle GoldenGate Stream Analytics, versions 19.1.0.0.0-19.1.0.0.14
- Oracle GraalVM Enterprise Edition, version 21.3.17
- Oracle GraalVM for JDK, versions 17.0.18, 21.0.10
- Oracle Graph Server and Client, versions 24.4.5, 25.4.1, 26.1.0
- Oracle Hospitality Cruise Shipboard Property Management (SPMS), versions 23.1.5-23.3.0
- Oracle HTTP Server, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Hyperion Infrastructure Technology, version 11.2.24.0.0
- Oracle Identity Manager, versions 12.2.1.4.0, 14.1.2.0.0, 14.1.2.1.0
- Oracle Identity Manager Connector, version 12.2.1.4.0

- Oracle Insurance Policy Administration J2EE, versions 11.3.1.0, 11.3.2.0, 12.0.5.0, 12.1.1.0
- Oracle Insurance Policy Administration Operational Data Store for Life and Annuity, version 1.0.2.1
- Oracle Java SE, versions 8u481, 8u481-b50, 8u481-perf, 11.0.30, 17.0.18, 21.0.10, 25.0.1, 25.0.2, 26
- Oracle Life Sciences Empirica Signal, versions 9.2.1-9.2.3
- Oracle Life Sciences InForm, versions 7.0.1.0, 7.0.1.1
- Oracle Managed File Transfer, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Middleware Common Libraries and Tools, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle NoSQL Database, versions 1.6.5, 1.7.0
- Oracle Outside In Technology, version 8.5.8
- Oracle Product Lifecycle Analytics, version 3.6.1
- Oracle REST Data Services, versions 24.2.0, 24.2.1, 24.3.0, 24.3.1, 24.4.0, 25.1.1, 25.2.0, 25.2.1, 25.2.2, 25.2.3, 25.3.0, 25.3.1, 25.4.0
- Oracle Retail Assortment Planning, versions 15.0, 16.0
- Oracle Retail Bulk Data Integration, versions 16.0.3, 19.0.1
- Oracle Retail EFTLink, versions 21.0.0-25.0.0
- Oracle Retail Extract Tranform and Load, version 13.0.5
- Oracle Retail Financial Integration, versions 16.0.3, 19.0.1
- Oracle Retail Fiscal Management, version 14.2
- Oracle Retail Integration Bus, versions 16.0.3, 19.0.1
- Oracle Retail Merchandise Financial Planning, versions 15.0, 16.0
- Oracle Retail Merchandising System, versions 16.0.3, 19.0.1
- Oracle Retail Predictive Application Server, version 16.0.3
- Oracle Retail Price Management, version 16.0.3
- Oracle Retail Service Backbone, versions 16.0.3, 19.0.1
- Oracle Retail Warehouse Management System, version 16.0
- Oracle Retail Xstore Point of Service, versions 21.0.5, 22.0.3
- Oracle Security Service, versions 12.1.3.0.0, 12.2.1.4.0
- Oracle SOA Suite, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Solaris, version 11.4
- Oracle TimesTen In-Memory Database, versions 18.1.4, 22.1.1
- Oracle Tuxedo, versions 22.1.0, 22.1.1

- Oracle Utilities Application Framework, versions 4.3.0.5.0-4.3.0.6.0, 4.4.0.0.0-4.4.0.4.0, 4.5.0.0.0-4.5.0.2.0, 25.4, 25.10, 26.4
- Oracle Utilities Live Energy Connect, versions 7.1.0.0.45, 25.12.0.0.0
- Oracle Utilities Network Management System, versions 2.4.0.1.31, 2.5.0.1.16, 2.5.0.2.10, 2.6.0.1.10, 2.6.0.2.5, 2.6.0.2.6
- Oracle Utilities Testing Accelerator, versions 7.0.0.0.7, 7.0.0.1.5, 25.4.0.0.2
- Oracle VM VirtualBox, version 7.2.6
- Oracle Web Services Manager, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle WebCenter Forms Recognition, version 14.1.1.0.0
- Oracle WebCenter Sites, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle WebLogic Server, versions 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0, 15.1.1.0.0
- PeopleSoft Enterprise CC Common Application Objects, version 9.2
- PeopleSoft Enterprise CS Student Records, version 9.2
- PeopleSoft Enterprise FIN Contracts, version 9.2
- PeopleSoft Enterprise FIN Maintenance Management, version 9.2
- PeopleSoft Enterprise FIN Project Costing, version 9.2
- PeopleSoft Enterprise HCM Absence Management, version 9.2
- PeopleSoft Enterprise HCM Human Resources, version 9.2
- PeopleSoft Enterprise HCM Shared Components, version 9.2
- PeopleSoft Enterprise PeopleTools, versions 8.61-8.62
- PeopleSoft Enterprise SCM Purchasing, version 9.2
- Primavera P6 Enterprise Project Portfolio Management, versions 21.12.0.0-21.12.21.6, 22.12.0.0-22.12.21.1, 23.12.0.0-23.12.18.0, 24.12.0.0-24.12.13.0, 25.12.0.0-25.12.2.0
- Primavera Unifier, versions 21.12.0-21.12.17, 22.12.0-22.12.15, 23.12.0-23.12.16, 24.12.0-24.12.13, 25.12.0-25.12.3
- Siebel Applications, versions 17.0-26.2
- Sun ZFS Storage Appliance Kit, version 8.8

Identificateurs externes

- CVE-2026-35252 CVE-2026-35251 CVE-2026-35250 CVE-2026-35249 CVE-2026-35248
- CVE-2026-35247 CVE-2026-35246 CVE-2026-35245 CVE-2026-35244 CVE-2026-35243
- CVE-2026-35242 CVE-2026-35241 CVE-2026-35240 CVE-2026-35239 CVE-2026-35238
- CVE-2026-35237 CVE-2026-35236 CVE-2026-35235 CVE-2026-35234 CVE-2026-35232
- CVE-2026-35231 CVE-2026-35230 CVE-2026-35229 CVE-2026-34325 CVE-2026-34324
- CVE-2026-34323 CVE-2026-34321 CVE-2026-34320 CVE-2026-34319 CVE-2026-34318

- CVE-2026-34317 CVE-2026-34315 CVE-2026-34314 CVE-2026-34313 CVE-2026-34312
- CVE-2026-34310 CVE-2026-34309 CVE-2026-34308 CVE-2026-34307 CVE-2026-34306
- CVE-2026-34305 CVE-2026-34304 CVE-2026-34303 CVE-2026-34302 CVE-2026-34301
- CVE-2026-34300 CVE-2026-34299 CVE-2026-34298 CVE-2026-34297 CVE-2026-34296
- CVE-2026-34295 CVE-2026-34294 CVE-2026-34293 CVE-2026-34292 CVE-2026-34291
- CVE-2026-34290 CVE-2026-34289 CVE-2026-34288 CVE-2026-34287 CVE-2026-34286
- CVE-2026-34285 CVE-2026-34284 CVE-2026-34283 CVE-2026-34282 CVE-2026-34281
- CVE-2026-34280 CVE-2026-34279 CVE-2026-34278 CVE-2026-34277 CVE-2026-34276
- CVE-2026-34275 CVE-2026-34274 CVE-2026-34273 CVE-2026-34272 CVE-2026-34271
- CVE-2026-34270 CVE-2026-34269 CVE-2026-34268 CVE-2026-34267 CVE-2026-34266
- CVE-2026-34237 CVE-2026-33870 CVE-2026-33013 CVE-2026-3288 CVE-2026-31790
- CVE-2026-30936 CVE-2026-30935 CVE-2026-30931 CVE-2026-30929 CVE-2026-30883
- CVE-2026-28693 CVE-2026-28692 CVE-2026-28691 CVE-2026-28690 CVE-2026-28689
- CVE-2026-28688 CVE-2026-28687 CVE-2026-28686 CVE-2026-28494 CVE-2026-28493
- CVE-2026-27830 CVE-2026-27799 CVE-2026-27798 CVE-2026-27727 CVE-2026-27135
- CVE-2026-27100 CVE-2026-27099 CVE-2026-26983 CVE-2026-26284 CVE-2026-26283
- CVE-2026-26066 CVE-2026-26007 CVE-2026-25990 CVE-2026-25989 CVE-2026-25988
- CVE-2026-25987 CVE-2026-25986 CVE-2026-25985 CVE-2026-25983 CVE-2026-25982
- CVE-2026-25971 CVE-2026-25970 CVE-2026-25969 CVE-2026-25968 CVE-2026-25967
- CVE-2026-25966 CVE-2026-25965 CVE-2026-25898 CVE-2026-25897 CVE-2026-25799
- CVE-2026-25798 CVE-2026-25797 CVE-2026-25796 CVE-2026-25795 CVE-2026-25794
- CVE-2026-25646 CVE-2026-25638 CVE-2026-25637 CVE-2026-25576 CVE-2026-25210
- CVE-2026-24734 CVE-2026-24733 CVE-2026-24515 CVE-2026-24514 CVE-2026-24513
- CVE-2026-24512 CVE-2026-24485 CVE-2026-24484 CVE-2026-24481 CVE-2026-24400
- CVE-2026-23903 CVE-2026-23901 CVE-2026-23865 CVE-2026-23864 CVE-2026-23490
- CVE-2026-22801 CVE-2026-22796 CVE-2026-22795 CVE-2026-22695 CVE-2026-22444
- CVE-2026-22184 CVE-2026-22022 CVE-2026-22021 CVE-2026-22019 CVE-2026-22018
- CVE-2026-22017 CVE-2026-22016 CVE-2026-22015 CVE-2026-22014 CVE-2026-22013
- CVE-2026-22011 CVE-2026-22010 CVE-2026-22009 CVE-2026-22008 CVE-2026-22007
- CVE-2026-22006 CVE-2026-22005 CVE-2026-22004 CVE-2026-22003 CVE-2026-22002
- CVE-2026-22001 CVE-2026-21999 CVE-2026-21998 CVE-2026-21997 CVE-2026-21992
- CVE-2026-21969 CVE-2026-21947 CVE-2026-21945 CVE-2026-21939 CVE-2026-21933
- CVE-2026-21932 CVE-2026-21925 CVE-2026-21637 CVE-2026-21636 CVE-2026-21452

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – 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 ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- CVE-2026-21441 CVE-2026-20676 CVE-2026-20652 CVE-2026-20644 CVE-2026-20636
- CVE-2026-20635 CVE-2026-20608 CVE-2026-1642 CVE-2026-1580 CVE-2026-0915
- CVE-2026-0861 CVE-2026-0540 CVE-2025-9900 CVE-2025-9670 CVE-2025-9232
- CVE-2025-9231 CVE-2025-9230 CVE-2025-9086 CVE-2025-8961 CVE-2025-8916
- CVE-2025-8885 CVE-2025-8869 CVE-2025-8194 CVE-2025-8177 CVE-2025-8176
- CVE-2025-8058 CVE-2025-7962 CVE-2025-7425 CVE-2025-6965 CVE-2025-69421
- CVE-2025-69420 CVE-2025-69419 CVE-2025-69418 CVE-2025-69230 CVE-2025-69229
- CVE-2025-69228 CVE-2025-69227 CVE-2025-69226 CVE-2025-69225 CVE-2025-69224
- CVE-2025-69223 CVE-2025-68973 CVE-2025-68615 CVE-2025-68431 CVE-2025-68161
- CVE-2025-68160 CVE-2025-68121 CVE-2025-67779 CVE-2025-67735 CVE-2025-67721
- CVE-2025-67639 CVE-2025-67638 CVE-2025-67637 CVE-2025-67636 CVE-2025-67635
- CVE-2025-66614 CVE-2025-66566 CVE-2025-66516 CVE-2025-66471 CVE-2025-66453
- CVE-2025-66418 CVE-2025-66293 CVE-2025-66200 CVE-2025-65082 CVE-2025-65018
- CVE-2025-64775 CVE-2025-64720 CVE-2025-64506 CVE-2025-64505 CVE-2025-6395
- CVE-2025-62728 CVE-2025-61984 CVE-2025-61795 CVE-2025-61732 CVE-2025-61729
- CVE-2025-61727 CVE-2025-61725 CVE-2025-61724 CVE-2025-61723 CVE-2025-6069
- CVE-2025-6052 CVE-2025-6021 CVE-2025-5987 CVE-2025-59775 CVE-2025-59476
- CVE-2025-59475 CVE-2025-59474 CVE-2025-59466 CVE-2025-59465 CVE-2025-59419
- CVE-2025-58754 CVE-2025-58189 CVE-2025-58188 CVE-2025-58187 CVE-2025-58186
- CVE-2025-58185 CVE-2025-58183 CVE-2025-58181 CVE-2025-58098 CVE-2025-58057
- CVE-2025-58056 CVE-2025-58050 CVE-2025-55754 CVE-2025-55753 CVE-2025-55184
- CVE-2025-55183 CVE-2025-55182 CVE-2025-55163 CVE-2025-55132 CVE-2025-55131
- CVE-2025-55130 CVE-2025-54571 CVE-2025-5449 CVE-2025-54090 CVE-2025-53864
- CVE-2025-5372 CVE-2025-53643 CVE-2025-5351 CVE-2025-5318 CVE-2025-52999
- CVE-2025-52967 CVE-2025-5115 CVE-2025-48976 CVE-2025-48924 CVE-2025-48913
- CVE-2025-48795 CVE-2025-4878 CVE-2025-4877 CVE-2025-48734 CVE-2025-47914
- CVE-2025-47912 CVE-2025-47910 CVE-2025-47436 CVE-2025-47219 CVE-2025-46762
- CVE-2025-46392 CVE-2025-4517 CVE-2025-4435 CVE-2025-43967 CVE-2025-43966
- CVE-2025-43457 CVE-2025-43368 CVE-2025-4330 CVE-2025-4138 CVE-2025-41254
- CVE-2025-41253 CVE-2025-41249 CVE-2025-41248 CVE-2025-41242 CVE-2025-35036
- CVE-2025-33042 CVE-2025-32990 CVE-2025-32989 CVE-2025-32988 CVE-2025-31948
- CVE-2025-31672 CVE-2025-30065 CVE-2025-29482 CVE-2025-27821 CVE-2025-27820
- CVE-2025-27818 CVE-2025-27817 CVE-2025-27636 CVE-2025-27210 CVE-2025-27209

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – 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 ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- CVE-2025-26791 CVE-2025-26333 CVE-2025-25193 CVE-2025-24970 CVE-2025-23184
- CVE-2025-22869 CVE-2025-22233 CVE-2025-1948 CVE-2025-15467 CVE-2025-15284
- CVE-2025-15224 CVE-2025-15079 CVE-2025-14819 CVE-2025-14524 CVE-2025-14279
- CVE-2025-14104 CVE-2025-14017 CVE-2025-13601 CVE-2025-13151 CVE-2025-13034
- CVE-2025-12543 CVE-2025-12383 CVE-2025-12183 CVE-2025-11201 CVE-2025-11200
- CVE-2025-11187 CVE-2025-11143 CVE-2025-10148 CVE-2025-0725 CVE-2025-0453
- CVE-2024-9287 CVE-2024-8184 CVE-2024-7254 CVE-2024-6763 CVE-2024-6387
- CVE-2024-56406 CVE-2024-5535 CVE-2024-52046 CVE-2024-51504 CVE-2024-47535
- CVE-2024-45339 CVE-2024-43394 CVE-2024-41172 CVE-2024-3884 CVE-2024-38820
- CVE-2024-37059 CVE-2024-36124 CVE-2024-34447 CVE-2024-32007 CVE-2024-31573
- CVE-2024-30172 CVE-2024-29857 CVE-2024-29736 CVE-2024-29371 CVE-2024-28752
- CVE-2024-24790 CVE-2024-24789 CVE-2024-23944 CVE-2024-13009 CVE-2024-12718
- CVE-2023-5388 CVE-2023-52428 CVE-2023-51775 CVE-2023-48795 CVE-2023-46750
- CVE-2023-44981 CVE-2023-3894 CVE-2023-35116 CVE-2023-34453 CVE-2023-34035
- CVE-2023-34034 CVE-2023-2976 CVE-2023-26464 CVE-2023-20863 CVE-2023-20862
- CVE-2023-1436 CVE-2022-46337 CVE-2022-45693 CVE-2022-45688 CVE-2022-45685
- CVE-2022-45047 CVE-2022-40150 CVE-2022-40149 CVE-2022-23307 CVE-2022-23305
- CVE-2022-23302 CVE-2021-45046 CVE-2021-28168 CVE-2021-22573 CVE-2021-0341
- CVE-2020-17521

Bilan de la vulnérabilité

Oracle a publié son Critical Patch Update (CPU) d’avril 2026, corrigeant plusieurs vulnérabilités critiques affectant les produits susmentionnés.

Certaines de ces vulnérabilités sont critiques et peuvent être exploitées à distance, parfois sans authentification, affectant notamment des composants exposés tels que les services web, middleware et applications d’entreprise.

L’exploitation de ces failles peut permettre une exécution de code arbitraire, une élévation de privilèges, un accès non autorisé aux données sensibles, un contournement de la politique de sécurité, un déni de service (DoS) sur les systèmes Oracle ou une compromission total du système affecté.

Solution

Veuillez se référer au bulletin de sécurité Oracle du 22 Avril 2026, 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 22 Avril 2026**:**

- https://www.oracle.com/security-alerts/cpuapr2026.html

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – 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 ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma