



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	60202101/26
Date de Publication	21 janvier 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- JD Edwards EnterpriseOne Tools, versions 9.2.0.0-9.2.26.0
- MySQL Cluster, versions 7.6.0-7.6.36, 8.0.0-8.0.44, 8.4.0-8.4.7, 9.0.0-9.5.0
- MySQL Connectors, versions 9.0.0-9.5.0
- MySQL Enterprise Backup, versions 8.0.0-8.0.44, 8.4.0-8.4.7, 9.0.0-9.5.0
- MySQL Server, versions 8.0.0-8.0.44, 8.4.0-8.4.7, 9.0.0-9.5.0
- MySQL Workbench, versions 8.0.0-8.0.45
- Oracle Access Manager, versions 12.2.1.4.0, 14.1.2.1.0
- Oracle Agile PLM, version 9.3.6
- Oracle Agile Product Lifecycle Management for Process, version 6.2.4
- Oracle APEX Sample Applications, versions 23.2.0, 23.2.1, 24.1.0, 24.2.0, 24.2.1
- Oracle Application Testing Suite, version 13.3.0.1
- Oracle Autovue for Agile Product Lifecycle Management, version 21.1.0
- Oracle AutoVue Office, version 21.1.0
- Oracle Banking Branch, versions 14.5.0.0.0, 14.6.0.0.0, 14.7.0.0.0, 14.8.0.0.0
- Oracle Banking Cash Management, versions 14.5.0.15.0, 14.6.0.11.0, 14.7.0.9.0, 14.8.0.1.0, 14.8.1.0.0
- Oracle Banking Corporate Lending Process Management, versions 14.5.0.0.0, 14.6.0.0.0, 14.7.0.0.0
- Oracle Banking Liquidity Management, versions 14.5.0.14.0, 14.5.0.15.0, 14.6.0.11.0, 14.7.0.9.0, 14.8.0.1.0, 14.8.1.0.0
- Oracle Banking Supply Chain Finance, versions 14.5.0.15.0, 14.6.0.11.0, 14.7.0.9.0, 14.8.0.1.0, 14.8.1.0.0
- 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 Business Process Management Suite, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Cloud Native Session Border Controller, version 25.1.0
- Oracle Coherence, versions 12.2.1.4.0, 14.1.1.0.0

- Oracle Commerce Guided Search, version 11.4.0
- Oracle Commerce Platform, version 11.4.0
- Oracle Communications ASAP, versions 7.4.0, 7.4.1
- Oracle Communications Billing and Revenue Management, versions 15.0.0.0.0, 15.0.1.0.0, 15.1.0.0.0
- Oracle Communications BRM - Elastic Charging Engine, versions 15.0.0.0, 15.0.1.0, 15.1.0.0
- Oracle Communications Diameter Signaling Router, versions 9.0.0, 9.0.1, 9.1.0
- Oracle Communications Element Manager, versions 9.0.0-9.0.4
- Oracle Communications IP Service Activator, version 7.5.0
- Oracle Communications Network Analytics Data Director, versions 24.2.0-24.2.1, 24.3.0, 25.1.100, 25.1.200, 25.2.100
- Oracle Communications Network Integrity, versions 7.3.6, 7.4.0, 7.5.0, 8.0.0
- 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 Policy Management, version 15.0.0.0
- Oracle Communications Pricing Design Center, versions 15.0.0.0.0, 15.0.1.0.0, 15.1.0.0.0
- Oracle Communications Session Border Controller, versions 9.3.0, 10.0.0
- Oracle Communications Session Report Manager, versions 9.0.0-9.0.4
- Oracle Communications Unified Assurance, versions 6.1.0-6.1.1
- Oracle Communications Unified Inventory Management, versions 7.7.0, 7.8.0, 8.0.0
- Oracle Data Integrator, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Database Server, versions 19.3-19.29, 21.3-21.20, 23.4.0-23.26.0
- Oracle E-Business Suite, versions 12.2.3-12.2.15
- Oracle Enterprise Communications Broker, versions 4.1.0, 4.2.0, 5.0.0
- Oracle Enterprise Manager Base Platform, versions 13.5, 24.1
- Oracle Essbase, version 21.8.0.0.0
- Oracle Financial Services Compliance Studio, version 2.6.0
- Oracle Financial Services Model Management and Governance, version 8.1.3.2
- Oracle FLEXCUBE Investor Servicing, versions 14.5.0.15.0, 14.7.0.8.0, 14.8.0.1.0
- Oracle FLEXCUBE Universal Banking, versions 14.0.0.0.0-14.8.0.0.0
- Oracle Fusion Middleware, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Global Lifecycle Management NextGen OUI Framework, version 15.1.1.0.0
- Oracle GoldenGate, versions 19.1.0.0.0-19.29.0.0.251021, 21.3-21.20, 23.4-23.10
- Oracle GoldenGate Big Data and Application Adapters, versions 19.1.0.0.0-19.1.0.0.20, 21.3-21.20, 23.4-23.10
- Oracle GoldenGate Stream Analytics, versions 19.1.0.0.0-19.1.0.0.13
- Oracle GoldenGate Studio, versions 23.8.0-23.9.0
- Oracle GoldenGate Veridata, versions 12.2.1.4.0-12.2.1.4.250531
- Oracle GraalVM Enterprise Edition, version 21.3.16
- Oracle GraalVM for JDK, versions 17.0.17, 21.0.9
- Oracle Graph Server and Client, versions 24.4.4, 25.4.0
- Oracle Health Sciences Information Manager, version 4.0.0
- Oracle Healthcare Data Repository, versions 8.2.0.5, 8.2.0.6
- Oracle Healthcare Master Person Index, versions 5.0.0.0-5.0.9.5
- Oracle Hospitality OPERA 5 Property Services, versions 5.6.19, 5.6.25, 5.6.26, 5.6.27
- Oracle HTTP Server, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in, versions 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0
- Oracle Hyperion Calculation Manager, version 11.2.23

- Oracle Hyperion Financial Close Management, version 11.2.23
- Oracle Hyperion Financial Management, version 11.2.23
- Oracle Hyperion Financial Reporting, version 11.2.23
- Oracle Hyperion Infrastructure Technology, version 11.2.23
- Oracle Hyperion Planning, version 11.2.23
- Oracle Hyperion Profitability and Cost Management, version 11.2.23
- Oracle Identity Manager, versions 12.2.1.4.0, 14.1.2.1.0
- Oracle Identity Manager Connector, versions 12.2.1.4.0, 14.1.2.1.0
- Oracle Insurance Policy Administration J2EE, versions 11.3.1-12.0.6
- Oracle Java SE, versions 8u471, 8u471-b50, 8u471-perf, 11.0.29, 17.0.17, 21.0.9, 25.0.1
- Oracle JDK Mission Control, version 9.1.1
- Oracle Key Vault, versions 21.1.0.0.0-21.11.0.0.0
- Oracle Life Sciences Central Coding, version 7.0.1.0
- Oracle Life Sciences Central Designer, version 7.0.1.0
- 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 1.5, 1.6
- Oracle Outside In Technology, versions 8.5.7, 8.5.8
- Oracle Planning and Budgeting Cloud Service, version 25.4.7
- Oracle Retail Advanced Inventory Planning, versions 15.0.3, 16.0.3
- Oracle Retail Allocation, versions 15.0.3, 16.0.3
- Oracle Retail Bulk Data Integration, versions 16.0.3, 19.0.1
- 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 Predictive Application Server, versions 15.0.3, 16.0.3
- Oracle Retail Service Backbone, versions 16.0.3, 19.0.1
- Oracle Retail Xstore Office, version 25.0.1
- 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, versions 19.1.0.0.0-19.1.0.1.0
- Oracle Security Service, version 12.2.1.4.0
- Oracle Service Bus, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle SOA Suite, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Solaris, versions 10, 11
- Oracle TimesTen In-Memory Database, versions 22.1.1.1.0-22.1.1.35.0
- Oracle Unified Directory, versions 12.2.1.4.0, 14.1.2.1.0
- 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, 25.4, 25.10
- Oracle Utilities Network Management System, versions 2.5.0.1.16, 2.5.0.2.10, 2.6.0.1.9, 2.6.0.2.5
- Oracle Utilities Testing Accelerator, versions 7.0.0.0.6, 7.0.0.1.4, 25.4.0.0.1
- Oracle VM VirtualBox, versions 7.1.14, 7.2.4
- Oracle WebCenter Enterprise Capture, versions 12.2.1.4.0, 14.1.2.0.0
- 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
- Oracle Weblogic Server Proxy Plug-in, versions 12.2.1.4.0, 14.1.1.0.0
- Oracle Zero Data Loss Recovery Appliance Software, versions 23.1.0-23.1.202509
- Oracle ZFS Storage Appliance Kit, version 8.8
- PeopleSoft Enterprise HCM Human Resources, version 9.2
- PeopleSoft Enterprise PeopleTools, versions 8.60, 8.61, 8.62

- PeopleSoft Enterprise SCM Purchasing, version 9.2
- Primavera Gateway, versions 21.12.0-21.12.16
- Primavera P6 Enterprise Project Portfolio Management, versions 21.12.0.0-21.12.21.5, 22.12.0.0-22.12.20.0, 23.12.0.0-23.12.17.0, 24.12.0.0-24.12.11.0
- Primavera Unifier, versions 21.12.0-21.12.17, 22.12.0-22.12.15, 23.12.0-23.12.16, 24.12.0-24.12.12, 25.12.0
- Service Delivery Platform, version 14.1.2.0.0
- Siebel Applications, versions 17.0-25.11

Identificateurs externes

CVE-2018-1000632 CVE-2020-10683 CVE-2021-23926 CVE-2021-33813 CVE-2021-43113
 CVE-2021-45105 CVE-2022-23395 CVE-2022-40196 CVE-2022-41342 CVE-2022-45047
 CVE-2023-1393 CVE-2023-29081 CVE-2023-4091 CVE-2023-4154 CVE-2023-42669
 CVE-2023-42670 CVE-2023-6378 CVE-2024-12133 CVE-2024-13009 CVE-2024-23337
 CVE-2024-23807 CVE-2024-30171 CVE-2024-31141 CVE-2024-35195 CVE-2024-42516
 CVE-2024-43204 CVE-2024-43796 CVE-2024-45720 CVE-2024-46901 CVE-2024-47252
 CVE-2024-47554 CVE-2024-51504 CVE-2024-52046 CVE-2024-56406 CVE-2024-57699
 CVE-2024-6763 CVE-2025-10148 CVE-2025-10911 CVE-2025-12183 CVE-2025-12383
 CVE-2025-12816 CVE-2025-13836 CVE-2025-13837 CVE-2025-22228 CVE-2025-22233
 CVE-2025-23048 CVE-2025-23084 CVE-2025-25193 CVE-2025-26333 CVE-2025-26791
 CVE-2025-27152 CVE-2025-27209 CVE-2025-27210 CVE-2025-27363 CVE-2025-27533
 CVE-2025-27817 CVE-2025-27818 CVE-2025-30065 CVE-2025-31672 CVE-2025-32988
 CVE-2025-32989 CVE-2025-32990 CVE-2025-41234 CVE-2025-41242 CVE-2025-41248
 CVE-2025-41249 CVE-2025-43272 CVE-2025-43342 CVE-2025-43356 CVE-2025-43368
 CVE-2025-43966 CVE-2025-43967 CVE-2025-4575 CVE-2025-46727 CVE-2025-46817
 CVE-2025-46818 CVE-2025-46819 CVE-2025-47183 CVE-2025-47219 CVE-2025-47910
 CVE-2025-47947 CVE-2025-48060 CVE-2025-48734 CVE-2025-4877 CVE-2025-4878
 CVE-2025-48795 CVE-2025-48866 CVE-2025-48924 CVE-2025-48976 CVE-2025-48989
 CVE-2025-4949 CVE-2025-49794 CVE-2025-49795 CVE-2025-49796 CVE-2025-49812
 CVE-2025-49844 CVE-2025-50059 CVE-2025-5115 CVE-2025-52520 CVE-2025-52891
 CVE-2025-52999 CVE-2025-5318 CVE-2025-5351 CVE-2025-53547 CVE-2025-53643
 CVE-2025-5372 CVE-2025-53864 CVE-2025-5449 CVE-2025-54571 CVE-2025-54874
 CVE-2025-54988 CVE-2025-55039 CVE-2025-55163 CVE-2025-55753 CVE-2025-55754
 CVE-2025-58056 CVE-2025-58057 CVE-2025-58098 CVE-2025-58754 CVE-2025-59250
 CVE-2025-59375 CVE-2025-59419 CVE-2025-59775 CVE-2025-5987 CVE-2025-6021
 CVE-2025-6052 CVE-2025-6069 CVE-2025-6075 CVE-2025-61755 CVE-2025-61795
 CVE-2025-6395 CVE-2025-64505 CVE-2025-64506 CVE-2025-64718 CVE-2025-64720
 CVE-2025-65018 CVE-2025-65082 CVE-2025-66200 CVE-2025-66418 CVE-2025-66471
 CVE-2025-66516 CVE-2025-66566 CVE-2025-67735 CVE-2025-68161 CVE-2025-6965
 CVE-2025-7424 CVE-2025-7425 CVE-2025-7962 CVE-2025-8176 CVE-2025-8177
 CVE-2025-8194 CVE-2025-8291 CVE-2025-8732 CVE-2025-8869 CVE-2025-8885
 CVE-2025-8916 CVE-2025-8961 CVE-2025-9086 CVE-2025-9230 CVE-2025-9231
 CVE-2025-9232 CVE-2025-9900 CVE-2026-21922 CVE-2026-21923 CVE-2026-21924
 CVE-2026-21925 CVE-2026-21926 CVE-2026-21927 CVE-2026-21928 CVE-2026-21929
 CVE-2026-21930 CVE-2026-21931 CVE-2026-21932 CVE-2026-21933 CVE-2026-21934
 CVE-2026-21935 CVE-2026-21936 CVE-2026-21937 CVE-2026-21938

CVE-2026-21939	CVE-2026-21940	CVE-2026-21941	CVE-2026-21942	CVE-2026-21943
CVE-2026-21944	CVE-2026-21945	CVE-2026-21946	CVE-2026-21947	CVE-2026-21948
CVE-2026-21949	CVE-2026-21950	CVE-2026-21951	CVE-2026-21952	CVE-2026-21955
CVE-2026-21956	CVE-2026-21957	CVE-2026-21958	CVE-2026-21959	CVE-2026-21960
CVE-2026-21961	CVE-2026-21962	CVE-2026-21963	CVE-2026-21964	CVE-2026-21965
CVE-2026-21966	CVE-2026-21967	CVE-2026-21968	CVE-2026-21969	CVE-2026-21970
CVE-2026-21971	CVE-2026-21972	CVE-2026-21973	CVE-2026-21974	CVE-2026-21975
CVE-2026-21976	CVE-2026-21977	CVE-2026-21978	CVE-2026-21979	CVE-2026-21980
CVE-2026-21981	CVE-2026-21982	CVE-2026-21983	CVE-2026-21984	CVE-2026-21985
CVE-2026-21986	CVE-2026-21987	CVE-2026-21988	CVE-2026-21989	CVE-2026-21990

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, d'élever ses privilèges 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
- Elévation de privilèges
- Déni de service

Référence

Bulletin de sécurité d'Oracle :

- <https://www.oracle.com/security-alerts/cpujan2026.html>