AVIS DE SECURITE

Objet	Multiples vulnérabilités critiques dans les produits Oracle (Critical Security Patch Update - Septembre 2026)
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-201
TLP	WHITE

Résumé

Oracle a publié aujourd'hui sa Critical Security Patch Update (CSPU) de septembre 2026, qui comprend 714 nouveaux correctifs de sécurité couvrant l'ensemble du portefeuille de produits Oracle on-premises (Fusion Middleware, Hyperion, E-Business Suite, Siebel CRM, Enterprise Manager, Communications, Analytics, Database Server, PeopleSoft, Essbase, Supply Chain, Virtualization, et autres). Le score CVSS v3.1 le plus élevé confirmé est de 10.0, sur des composants d'Oracle Fusion Middleware (dont Oracle WebLogic Server, Oracle Access Manager, Oracle Identity Manager, Oracle Coherence) et d'Oracle Hyperion, avec un grand nombre de vulnérabilités exploitables à distance sans authentification. Oracle recommande l'application des correctifs dans les meilleurs délais. Les informations ci-dessous sont issues des résumés exécutifs publiés par Oracle ; les identifiants CVE individuels seront précisés dans la cartographie officielle publiée par l'éditeur.

Risque de sécurité

- Exécution de code arbitraire à distance / élévation de privilèges
- Atteinte à la confidentialité et à l'intégrité des données
- Contournement de la politique de sécurité

Systèmes affectés

- Oracle Fusion Middleware : WebLogic Server, Access Manager, Identity Manager, Coherence, Internet Directory, Web Services Manager, WebCenter Content/Portal/Sites/Enterprise Capture, Forms, JDeveloper, Data Integrator, Managed File Transfer, Helidon (versions 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0, 15.1.1.0.0 selon composant)
- Oracle Hyperion : Data Relationship Management, Financial Management, Profitability and Cost Management, version 11.2.26.0.0
- Oracle E-Business Suite, versions 12.2.3 à 12.2.15, et V16
- Oracle Siebel CRM (Siebel Applications), versions 17.0 à 26.7
- Oracle Enterprise Manager (Base Platform, for Fusion Middleware, for Oracle Database), versions 13.5 et 24.1
- Oracle Communications : Cloud Native Core Security Edge Protection Proxy, MetaSolv Solution, Operations Monitor, Service Catalog and Design, Unified Assurance
- Oracle Analytics : BI Publisher et Business Intelligence Enterprise Edition, versions 8.2.0.0.0, 12.2.1.4.0, 26.1.0.0.0
- Oracle Essbase, version 21.8.3.0.0
- Oracle Database Server, versions 19.3-19.32, 21.3-21.23, 23.4.0-23.26.3
- Oracle PeopleSoft : PeopleTools (8.61-8.63) et modules applicatifs associés
- Oracle Supply Chain : Agile PLM, Agile Engineering Data Management, Agile PLM MCAD Connector, Product

Lifecycle Analytics
- Oracle Virtualization : Oracle VM VirtualBox, version 7.2.16
- Autres produits affectés à un degré moindre (CVSS < 8.5) : Oracle Commerce, Oracle Java SE / GraalVM, Oracle Utilities Network Management System, Oracle Financial Services Applications (Banking), Oracle Autonomous Health Framework, Oracle Application Testing Suite

Recommandations

Se référer au bulletin de sécurité de l'éditeur du 15 septembre 2026 (Critical Security Patch Update - September 2026) :

- https://www.oracle.com/security-alerts/cspusep2026.html
- https://www.oracle.com/security-alerts/
- https://www.oracle.com/security-alerts/public-vuln-to-advisory-mapping.html