



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	50251710/24
Date de Publication	17 Octobre 2024
Risque	Important
Impact	Critique

Systèmes affectés

- Autonomous Health Framework, versions antérieures à 24.9
- GoldenGate Stream Analytics, versions 19.1.0.0.0-19.1.0.0.9
- Management Cloud Engine, version 24.1.0.0.0
- MySQL Client, versions 8.0.39 et antérieures, 8.4.2 et antérieures, 9.0.1 et antérieures
- MySQL Cluster, versions 7.5.35 et antérieures, 7.6.31 et antérieures, 8.0.39 et antérieures, 8.4.2 et antérieures, 9.0.1 et antérieures
- MySQL Connectors, versions 9.0.0 et antérieures
- MySQL Enterprise Backup, versions 8.0.39 et antérieures, 8.4.2 et antérieures, 9.0.1 et antérieures
- MySQL Enterprise Monitor, versions 8.0.39 et antérieures
- MySQL Server, versions 8.0.39 et antérieures, 8.4.2 et antérieures, 9.0.1 et antérieures
- MySQL Shell, versions 8.0.38 et antérieures, 8.4.1 et antérieures, 9.0.1 et antérieures
- MySQL Workbench, versions 8.0.38 et antérieures
- Oracle Access Manager, version 12.2.1.4.0
- Oracle Agile PLM, version 9.3.6
- Oracle Application Express, versions 23.1, 23.2, 24.1
- Oracle Application Testing Suite, version 13.3.0.1
- Oracle Autovue for Agile Product Lifecycle Management, version 21.1.0
- Oracle Banking APIs, versions 19.2.0.0.0, 21.1.0.0.0, 22.1.0.0.0, 22.2.0.0.0
- Oracle Banking Cash Management, versions 14.7.4.0.0, 14.7.5.0.0
- Oracle Banking Corporate Lending Process Management, versions 14.4.0.0.0, 14.5.0.0.0, 14.6.0.0.0, 14.7.0.0.0
- Oracle Banking Digital Experience, versions 19.2.0.0.0, 21.1.0.0.0, 22.1.0.0.0, 22.2.0.0.0
- Oracle Banking Liquidity Management, versions 14.5.0.12.0, 14.7.0.6.0, 14.7.4.0.0, 14.7.5.0.0
- Oracle Banking Supply Chain Finance, versions 14.7.4.0.0, 14.7.5.0.0
- Oracle BI Publisher, versions 7.0.0.0.0, 7.6.0.0.0, 12.2.1.4.0
- Oracle Blockchain Platform, version 21.1.2

- 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 Commerce Guided Search, versions 11.3.2, 11.4.0
- Oracle Commerce Platform, versions 11.3.0, 11.3.1, 11.3.2
- Oracle Communications ASAP, version 7.4.3.0.2
- Oracle Communications Cloud Native Core Automated Test Suite, versions 23.4.3, 23.4.4, 24.1.1, 24.2.2
- Oracle Communications Cloud Native Core Binding Support Function, versions 23.4.0-23.4.5
- Oracle Communications Cloud Native Core Certificate Management, versions 23.4.2, 23.4.3, 24.2.0
- Oracle Communications Cloud Native Core Console, versions 23.4.2, 24.2.0
- Oracle Communications Cloud Native Core DBTier, versions 24.1.0, 24.2.0
- Oracle Communications Cloud Native Core Network Function Cloud Native Environment, versions 23.4.0, 24.1.0-24.2.0
- Oracle Communications Cloud Native Core Network Repository Function, versions 23.4.4, 24.2.1
- Oracle Communications Cloud Native Core Network Slice Selection Function, versions 24.2.0, 24.2.1
- Oracle Communications Cloud Native Core Policy, versions 23.4.0-23.4.6
- Oracle Communications Cloud Native Core Security Edge Protection Proxy, versions 23.4.2, 24.2.0
- Oracle Communications Cloud Native Core Service Communication Proxy, versions 23.4.0, 24.1.0, 24.2.0
- Oracle Communications Cloud Native Core Unified Data Repository, version 24.2.0
- Oracle Communications Convergent Charging Controller, versions 6.0.1.0.0, 12.0.1.0.0-12.0.6.0.0, 15.0.0.0.0
- Oracle Communications Core Session Manager, version 9.1.5
- Oracle Communications EAGLE Application Processor, version 17.0.1
- Oracle Communications IP Service Activator, versions 7.4.0, 7.5.0
- Oracle Communications LSMS, version 14.0.0.1
- Oracle Communications Messaging Server, version 8.1
- Oracle Communications Network Analytics Data Director, versions 23.4.0, 24.1.0, 24.2.0
- Oracle Communications Network Charging and Control, versions 6.0.1.0.0, 12.0.1.0.0-12.0.6.0.0, 15.0.0.0.0
- 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 Performance Intelligence Center, versions antérieures à 10.4.0.4
- Oracle Communications Policy Management, versions 12.6.1.0.0, 15.0.0.0.0
- Oracle Communications Session Border Controller, versions 9.1.0, 9.2.0, 9.3.0
- Oracle Communications Unified Assurance, versions 5.5.0-5.5.22, 6.0.0-6.0.5
- Oracle Communications User Data Repository, versions 12.11.0, 14.0
- Oracle Data Integrator, version 12.2.1.4.0
- Oracle Database Server, versions 19.3-19.24, 21.3-21.15, 23.4-23.5
- Oracle E-Business Suite, versions 12.2.3-12.2.14, [ECC] 11-13
- Oracle Enterprise Communications Broker, versions 4.1.0, 4.2.0
- Oracle Enterprise Data Quality, version 12.2.1.4.0
- Oracle Enterprise Manager Base Platform, versions 12.2.1.4.0, 13.5.0.0
- Oracle Enterprise Manager for Fusion Middleware, version 12.2.1.4.0
- Oracle Enterprise Manager for Peoplesoft, version 13.5.1.1.0
- Oracle Enterprise Manager Fusion Middleware Control, version 12.2.1.4.0
- Oracle Enterprise Operations Monitor, versions 5.1, 5.2

- Oracle Essbase, version 21.6
- Oracle Financial Services Compliance Studio, versions 8.1.2.7, 8.1.2.8
- Oracle Financial Services Revenue Management and Billing, versions 3.0.0.0.0, 4.0.0.0.0, 5.0.0.0.0
- Oracle Global Lifecycle Management FMW Installer, version 12.2.1.4.0
- Oracle GoldenGate Big Data and Application Adapters, versions 19.1.0.0.0-19.1.0.0.9
- Oracle GraalVM Enterprise Edition, versions 20.3.15, 21.3.11
- Oracle GraalVM for JDK, versions 17.0.12, 21.0.4, 23
- Oracle Graph Server and Client, versions 23.4.3, 24.3.0
- Oracle Hospitality Cruise Shipboard Property Management System, version 23.1.3
- Oracle Hospitality OPERA 5, versions 5.6.19.19, 5.6.25.8, 5.6.26.4
- Oracle Hospitality Symphony, versions 19.1.0-19.6.2
- Oracle HTTP Server, versions 12.2.1.4.0, 14.1.1.0.0
- Oracle Hyperion BI+, version 11.2.18.0.0
- Oracle Hyperion Financial Management, version 11.2.18.0.0
- Oracle Hyperion Infrastructure Technology, version 11.2.18.0.0
- Oracle Identity Manager Connector, versions 11.1.1.5.0, 12.2.1.3.0
- Oracle Java SE, versions 8u421, 8u421-perf, 11.0.24, 17.0.12, 21.0.4, 23
- Oracle Managed File Transfer, version 12.2.1.4.0
- Oracle Middleware Common Libraries and Tools, version 12.2.1.4.0
- Oracle NoSQL Database, versions 1.5.0, 20.3.40, 21.2.71, 22.3.45, 23.3.33, 24.1.17
- Oracle Outside In Technology, version 8.5.7
- Oracle Retail Customer Management and Segmentation Foundation, version 19.0.0.10
- Oracle Retail EFTLink, versions 20.0.1, 21.0.0, 22.0.0, 23.0.0
- Oracle SD-WAN Aware, version 9.0.1.10.0
- Oracle SD-WAN Edge, versions 9.1.1.3.0, 9.1.1.5.0-9.1.1.8.0, 9.1.1.9.0
- Oracle Secure Backup, versions 18.1.0.1.0, 18.1.0.2.0, 19.1.0.0.0
- Oracle Service Bus, version 12.2.1.4.0
- Oracle Solaris Cluster, version 4
- Oracle SQL Developer, versions 23.1.0, 24.3.0
- Oracle Utilities Application Framework, versions 4.0.0.0.0, 4.0.0.2.0, 4.0.0.3.0, 4.3.0.3.0-4.3.0.6.0, 4.5.0.0.0
- Oracle Utilities Network Management System, versions 2.3.0.2.34, 2.4.0.1.25, 2.5.0.1.14, 2.5.0.2.8, 2.6.0.1.5
- Oracle VM VirtualBox, versions antérieures à 7.0.22, antérieures à 7.1.2
- Oracle WebCenter Forms Recognition, version 14.1.1.0.0
- Oracle WebCenter Portal, version 12.2.1.4.0
- Oracle WebCenter Sites, version 12.2.1.4.0
- Oracle WebLogic Server, versions 12.2.1.4.0, 14.1.1.0.0
- PeopleSoft Enterprise CC Common Application Objects, version 9.2
- PeopleSoft Enterprise ELM Enterprise Learning Management, version 9.2
- PeopleSoft Enterprise FIN Expenses, version 9.2
- PeopleSoft Enterprise HCM Global Payroll Core, versions 9.2.48-9.2.50
- PeopleSoft Enterprise PeopleTools, versions 8.59, 8.60, 8.61
- Siebel Applications, versions 24.7 et antérieures

Identificateurs externes

CVE-2019-10172	CVE-2020-11022	CVE-2020-11023	CVE-2020-13956	CVE-2020-14145
CVE-2020-15778	CVE-2020-17521	CVE-2020-8908	CVE-2020-9493	CVE-2021-23358
CVE-2021-28170	CVE-2021-36368	CVE-2021-36713	CVE-2021-37136	CVE-2021-37137
CVE-2021-41182	CVE-2021-41183	CVE-2021-41184	CVE-2022-1292	CVE-2022-1471
CVE-2022-2068	CVE-2022-23302	CVE-2022-23305	CVE-2022-23307	CVE-2022-23437
CVE-2022-2601	CVE-2022-31129	CVE-2022-31160	CVE-2022-34169	CVE-2022-34381
CVE-2022-36033	CVE-2022-36760	CVE-2022-37454	CVE-2022-38136	CVE-2022-3996
CVE-2022-40196	CVE-2022-41342	CVE-2022-4203	CVE-2022-42919	CVE-2022-4304
CVE-2022-4450	CVE-2022-45061	CVE-2022-46337	CVE-2023-0215	CVE-2023-0216
CVE-2023-0217	CVE-2023-0286	CVE-2023-0401	CVE-2023-20863	CVE-2023-26031
CVE-2023-26464	CVE-2023-26551	CVE-2023-26552	CVE-2023-26553	CVE-2023-26554
CVE-2023-26555	CVE-2023-27391	CVE-2023-28439	CVE-2023-28484	CVE-2023-28823
CVE-2023-29469	CVE-2023-2953	CVE-2023-2976	CVE-2023-33201	CVE-2023-34055
CVE-2023-34453	CVE-2023-34454	CVE-2023-34455	CVE-2023-35116	CVE-2023-3635
CVE-2023-37920	CVE-2023-38408	CVE-2023-38545	CVE-2023-39410	CVE-2023-39743
CVE-2023-4043	CVE-2023-42503	CVE-2023-42843	CVE-2023-42950	CVE-2023-42956
CVE-2023-43642	CVE-2023-44483	CVE-2023-44487	CVE-2023-44981	CVE-2023-45288
CVE-2023-45853	CVE-2023-46136	CVE-2023-4759	CVE-2023-4807	CVE-2023-4863
CVE-2023-48795	CVE-2023-49083	CVE-2023-50447	CVE-2023-5072	CVE-2023-51384
CVE-2023-51385	CVE-2023-51775	CVE-2023-52425	CVE-2023-52426	CVE-2023-52428
CVE-2023-5363	CVE-2023-5678	CVE-2023-5685	CVE-2023-5752	CVE-2023-6004
CVE-2023-6129	CVE-2023-6237	CVE-2023-6597	CVE-2023-6816	CVE-2023-6918
CVE-2023-7104	CVE-2024-0229	CVE-2024-0232	CVE-2024-0450	CVE-2024-0727
CVE-2024-1874	CVE-2024-21131	CVE-2024-21138	CVE-2024-21140	CVE-2024-21144
CVE-2024-21145	CVE-2024-21147	CVE-2024-21172	CVE-2024-21190	CVE-2024-21191
CVE-2024-21192	CVE-2024-21193	CVE-2024-21194	CVE-2024-21195	CVE-2024-21196
CVE-2024-21197	CVE-2024-21198	CVE-2024-21199	CVE-2024-21200	CVE-2024-21201
CVE-2024-21202	CVE-2024-21203	CVE-2024-21204	CVE-2024-21205	CVE-2024-21206
CVE-2024-21207	CVE-2024-21208	CVE-2024-21209	CVE-2024-21210	CVE-2024-21211
CVE-2024-21212	CVE-2024-21213	CVE-2024-21214	CVE-2024-21215	CVE-2024-21216
CVE-2024-21217	CVE-2024-21218	CVE-2024-21219	CVE-2024-21230	CVE-2024-21231
CVE-2024-21232	CVE-2024-21233	CVE-2024-21234	CVE-2024-21235	CVE-2024-21236
CVE-2024-21237	CVE-2024-21238	CVE-2024-21239	CVE-2024-21241	CVE-2024-21242
CVE-2024-21243	CVE-2024-21244	CVE-2024-21246	CVE-2024-21247	CVE-2024-21248
CVE-2024-21249	CVE-2024-21250	CVE-2024-21251	CVE-2024-21252	CVE-2024-21253
CVE-2024-21254	CVE-2024-21255	CVE-2024-21257	CVE-2024-21258	CVE-2024-21259
CVE-2024-21260	CVE-2024-21261	CVE-2024-21262	CVE-2024-21263	CVE-2024-21264
CVE-2024-21265	CVE-2024-21266	CVE-2024-21267	CVE-2024-21268	CVE-2024-21269
CVE-2024-21270	CVE-2024-21271	CVE-2024-21272	CVE-2024-21273	CVE-2024-21274
CVE-2024-21275	CVE-2024-21276	CVE-2024-21277	CVE-2024-21278	CVE-2024-21279
CVE-2024-21280	CVE-2024-21281	CVE-2024-21282	CVE-2024-21283	CVE-2024-21284
CVE-2024-21285	CVE-2024-21286	CVE-2024-21885	CVE-2024-21886	CVE-2024-22018
CVE-2024-22020	CVE-2024-22201	CVE-2024-22257	CVE-2024-22262	CVE-2024-23252
CVE-2024-23254	CVE-2024-23263	CVE-2024-23280	CVE-2024-23284	CVE-2024-23635
CVE-2024-23672	CVE-2024-23807	CVE-2024-23944	CVE-2024-2398	CVE-2024-2408

CVE-2024-24549	CVE-2024-24989	CVE-2024-24990	CVE-2024-25062	CVE-2024-2511
CVE-2024-25269	CVE-2024-25638	CVE-2024-25710	CVE-2024-26130	CVE-2024-26308
CVE-2024-27306	CVE-2024-27834	CVE-2024-27983	CVE-2024-28182	CVE-2024-28752
CVE-2024-28849	CVE-2024-28887	CVE-2024-29025	CVE-2024-29131	CVE-2024-29133
CVE-2024-2961	CVE-2024-29736	CVE-2024-29857	CVE-2024-30251	CVE-2024-31079
CVE-2024-31080	CVE-2024-31083	CVE-2024-31744	CVE-2024-32007	CVE-2024-32114
CVE-2024-32760	CVE-2024-33599	CVE-2024-33600	CVE-2024-33601	CVE-2024-33602
CVE-2024-33899	CVE-2024-34161	CVE-2024-34750	CVE-2024-35200	CVE-2024-36052
CVE-2024-36137	CVE-2024-36138	CVE-2024-36387	CVE-2024-3653	CVE-2024-37370
CVE-2024-37371	CVE-2024-37372	CVE-2024-37891	CVE-2024-38356	CVE-2024-38357
CVE-2024-38472	CVE-2024-38473	CVE-2024-38474	CVE-2024-38475	CVE-2024-38476
CVE-2024-38477	CVE-2024-38808	CVE-2024-38809	CVE-2024-38816	CVE-2024-38998
CVE-2024-38999	CVE-2024-39573	CVE-2024-39689	CVE-2024-39884	CVE-2024-40725
CVE-2024-40898	CVE-2024-41172	CVE-2024-41817	CVE-2024-41909	CVE-2024-43044
CVE-2024-43045	CVE-2024-43407	CVE-2024-43411	CVE-2024-45490	CVE-2024-45491
CVE-2024-45492	CVE-2024-4577	CVE-2024-45801	CVE-2024-4603	CVE-2024-4741
CVE-2024-5458	CVE-2024-5535	CVE-2024-5585	CVE-2024-5971	CVE-2024-6119
CVE-2024-6162	CVE-2024-6232	CVE-2024-6345	CVE-2024-6387	CVE-2024-7254
CVE-2024-7264	CVE-2024-7592	CVE-2024-7885		

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.

Un attaquant distant non authentifié peut exploiter ces vulnérabilités pour exécuter du code arbitraire, accéder à des données confidentielles ou causer un déni de service.

Solution

Veillez 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.
- Déni de service.

Référence

Bulletin de sécurité d'Oracle :

- <https://www.oracle.com/security-alerts/cpuoct2024.html>