DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 19-07-2025

BULLETIN ALERTES

Object	Multiples vulnérabilités dans les produits Oracle
Réference	1364
Date de Publication	2025-07-18
Sévérité	Critique

IMPACT :

- 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

SYSTÉME AFFECTÉ :

- Autonomous Health Framework, versions 24.11.0 à 25.4.0
- JD Edwards EnterpriseOne Tools, versions 9.2.0.0 à 9.2.9.3
- JD Edwards World Security, version A9.4
- MySQL Client, versions 8.0.0 à 8.0.42, 8.4.0 à 8.4.5, 9.0.0 à 9.3.0

- MySQL Cluster, versions 7.6.0 à 7.6.34, 8.0.0 à 8.0.42, 8.4.0 à 8.4.5, 9.0.0 à 9.3.0
- MySQL Enterprise Backup, versions 8.0.0 à 8.0.42, 8.4.0 à 8.4.5, 9.0.0 à 9.3.0
- MySQL Server, versions 8.0.0 à 8.0.42, 8.4.0 à 8.4.5, 9.0.0 à 9.3.0
- MySQL Workbench, versions 8.0.0 à 8.0.42
- Oracle Agile Engineering Data Management, version 6.2.1
- Oracle Agile PLM, version 9.3.6
- Oracle Application Express, versions 24.2.4, 24.2.5
- Oracle Application Testing Suite, version 13.3.0.1
- Oracle AutoVue, versions 21.0.2, 21.1.0
- Oracle Banking Origination, versions 14.4.0.0.0 à 14.7.0.0.0
- Oracle BI Publisher, versions 7.6.0.0.0, 8.2.0.0.0, 12.2.1.4.0
- Oracle Blockchain Platform, versions 21.4.3, 24.1.3
- 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 Coherence, versions 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0
- Oracle Commerce Guided Search, version 11.4.0
- Oracle Commerce Guided Search Platform Services, version 11.4.0
- Oracle Communications Billing and Revenue Management, versions 12.0.0.4 .0 à 12.0.0.8 .0, 15.0.0.0 .0, 15.0.1.0 .0, 15.1.0.0 .0
- Oracle Communications BRM à Elastic Charging Engine, versions 12.0.0.4 à 12.0.0.8 , 15.0.0.0 , 15.0.1.0 , 15.1.0.0
- Oracle Communications Calendar Server, version 8.0.0.8.0
- Oracle Communications Cloud Native Core Automated Test Suite, version 24.2.4
- Oracle Communications Cloud Native Core Binding Support Function, versions 24.2.0 à 24.2.3

- Oracle Communications Cloud Native Core Console, version 24.2.4
- Oracle Communications Cloud Native Core DBTier, versions 24.2.5, 24.3.0, 25.1.100
- Oracle Communications Cloud Native Core Network Data Analytics Function, versions 22.4.0, 23.1.0, 23.4.3
- Oracle Communications Cloud Native Core Network Exposure Function, version 24.2.0
- Oracle Communications Cloud Native Core Network Function Cloud Native Environment, version 25.1.100
- Oracle Communications Cloud Native Core Network Repository Function, version 24.2.4
- Oracle Communications Cloud Native Core Network Slice Selection Function, version 24.3.1
- Oracle Communications Cloud Native Core Policy, versions 24.2.0 à 24.2.6
- Oracle Communications Cloud Native Core Security Edge Protection Proxy, versions 24.2.4, 25.1.100, 25.1.101
- Oracle Communications Cloud Native Core Service Communication Proxy, versions 24.2.0, 25.1.100
- Oracle Communications Contacts Server, version 8.0.0.9.0
- Oracle Communications Convergence, versions 3.0.3.3.0, 3.0.3.4.0
- Oracle Communications Convergent Charging Controller, versions 12.0.3.0.0 à 12.0.6.0.0, 15.0.0.0 .0 à 15.0.1.0 .0, 15.1.0.0 .0
- Oracle Communications Core Session Manager, version 9.1.5
- Oracle Communications Element Manager, versions 9.0.0 à 9.0.4
- Oracle Communications IP Service Activator, versions 7.4.0, 7.5.0
- Oracle Communications MetaSolv Solution, version 6.3.1
- Oracle Communications Network Analytics Data Director, versions 24.2.0, 24.3.0, 25.1.100
- Oracle Communications Network Charging and Control, versions 12.0.3.0.0 à 12.0.6.0.0, 15.0.0.0 .0 à 15.0.1.0 .0, 15.1.0.0 .0
- Oracle Communications Network Integrity, versions 7.3.6, 7.4.0, 7.5.0

- Oracle Communications Offline Mediation Controller, versions 12.0.0.2 à 12.0.0.8 , 15.0.0.0 à 15.0.1.0
- 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 Policy Management, version 15.0.0.0
- Oracle Communications Session Border Controller, versions 9.2.0, 9.3.0, 10.0.0
- Oracle Communications Session Report Manager, versions 9.0.0 à 9.0.4
- Oracle Communications Unified Assurance, versions 6.0.5 à 6.1.0
- Oracle Communications Unified Inventory Management, versions 7.4.0 à 7.4.2, 7.5.0, 7.5.1, 7.6.0 à 7.8.0
- Oracle Communications User Data Repository, version 15.0.3
- Oracle Data Integrator, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Database Server, versions 19.3 à 19.27, 21.3 à 21.18, 23.4 à 23.8
- Oracle E à Business Suite, versions 12.2.3 à 12.2.14
- Oracle Enterprise Communications Broker, versions 4.1.0, 4.2.0, 5.0.0
- Oracle Enterprise Data Quality, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Essbase, version 21.7.2.0.0
- Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.7.8 , 8.0.8.5 , 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 Model Management and Governance, version 8.1.2.7
- Oracle Financial Services Trade à Based Anti Money Laundering Enterprise Edition, version 8.0.8
- Oracle Fusion Middleware, version 14.1.2.0.0
- Oracle GoldenGate Big Data and Application Adapters, versions 21.3 à 21.17, 23.4 à 23.7

- Oracle GoldenGate Stream Analytics, versions 19.1.0.0.0 à 19.1.0.0.11
- Oracle GoldenGate Studio, version 12.2.0.4.0
- Oracle GoldenGate Veridata, versions 12.2.1.4.0 à 12.2.1.4.250331
- Oracle GraalVM Enterprise Edition, version 21.3.14
- Oracle GraalVM for JDK, versions 17.0.15, 21.0.7, 24.0.1
- Oracle Graph Server and Client, versions 24.4.1, 25.1.0
- Oracle Healthcare Master Person Index, versions 5.0.0.0 à 5.0.9.2
- Oracle Hospitality Cruise Shipboard Property Management System, versions 23.1.4, 23.2.2
- Oracle HTTP Server, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle Hyperion Financial Reporting, version 11.2.20.0.0
- Oracle Hyperion Infrastructure Technology, version 11.2.21.0.0
- Oracle Identity Manager, version 12.2.1.4.0
- Oracle Insurance Policy Administration J2EE, versions 11.3.0 à 12.0.4
- Oracle Java SE, versions 8u451, 8u451 à b50, 8u451 à perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1
- Oracle JDeveloper, version 14.1.2.0.0
- Oracle Managed File Transfer, version 12.2.1.4.0
- Oracle Middleware Common Libraries and Tools, versions 12.2.1.4.0, 14.1.2.0.0
- Oracle NoSQL Database, versions 22.3.51, 23.1.38, 24.4.9
- Oracle Outside In Technology, version 8.5.7
- Oracle Product Lifecycle Analytics, version 3.6.1
- Oracle REST Data Services, versions 24.2.0, 24.4, 25.1.0
- Oracle Retail EFTLink, versions 20.0.1, 21.0.0, 22.0.0, 23.0.0
- Oracle Retail Extract Tranform and Load, version 13.2.5
- Oracle Retail Integration Bus, versions 14.1.3.2 , 15.0.3.1 , 16.0.3, 19.0.1

- Oracle Retail Predictive Application Server, versions 15.0.3, 16.0.3
- Oracle Retail Service Backbone, versions 14.1.3.2 , 15.0.3.1 , 16.0.3, 19.0.1
- Oracle Retail Xstore Office, versions 20.0.5, 21.0.4, 22.0.2, 23.0.2, 24.0.1
- Oracle Retail Xstore Point of Service, versions 20.0.5, 21.0.4, 22.0.2, 23.0.2, 24.0.1
- Oracle Service Bus, version 12.2.1.4.0
- Oracle Spatial Studio, version 24.1.0
- Oracle TimesTen In à Memory Database, versions 18.1.4.52.0, 22.1.1.32.0
- Oracle Utilities Application Framework, versions 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 à 24.3.0.0.0, 25.4
- Oracle Utilities Network Management System, versions 2.4.0.1.27, 2.5.0.1.15, 2.5.0.2.8, 2.5.0.2.9, 2.6.0.1.7, 2.6.0.2.1, 2.6.0.2.2
- Oracle Utilities Testing Accelerator, versions 7.0.0.0.0, 7.0.0.1.0
- Oracle VM VirtualBox, version 7.1.10
- Oracle WebCenter Enterprise Capture, version 12.2.1.4.0
- Oracle WebCenter Portal, version 12.2.1.4.0
- Oracle WebLogic Server, versions 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0
- PeopleSoft Enterprise HCM Global Payroll Core, versions 9.2.51, 9.2.52
- PeopleSoft Enterprise HCM Human Resources, version 9.2
- PeopleSoft Enterprise PeopleTools, versions 8.60, 8.61, 8.62
- Primavera P6 Enterprise Project Portfolio Management, versions 20.12.0 à 20.12.21, 21.12.0 à 21.12.21, 22.12.0 à 22.12.19, 23.12.0 à 23.12.13, 24.12.0 à 24.12.4
- Primavera Unifier, versions 20.12.0 à 20.12.16, 21.12.0 à 21.12.17, 22.12.0 à 22.12.15, 23.12.0 à 23.12.14, 24.12.0 à 24.12.6
- Siebel Applications, versions 25.0 à 25.5

DÉSCRIPTION :

Plusieurs vulnérabilités critiques ont été identifiées dans divers produits Oracle, comme en témoigne la mise à jour « Oracle Critical Patch Update » de juillet 2025. L’exploitation de certaines de ces vulnerablités pourrait permettre à un attaquant distant de prendre le contrôle total d’un système affecté, d’exécuter du code arbitraire, de contourner des politiques de sécurité, de provoquer un déni de service ou encore de compromettre la confidentialité des données.

SOLUTION :

Mettre à jour les produits Oracle. (se référer à la documentation)

DOCUMENTATION :

- Bulletin de sécurité Oracle du 16 Juillet 2025:

https://www.oracle.com/security-alerts/cpujul2025.html

- CVE-2020-13936 :

https://nvd.nist.gov/vuln/detail/cve-2020-13936

- CVE-2021-33813 :

https://nvd.nist.gov/vuln/detail/cve-2021-33813

- CVE-2021-42575 :

https://nvd.nist.gov/vuln/detail/cve-2021-42575

- CVE-2022-34169 :

https://nvd.nist.gov/vuln/detail/cve-2022-34169

- CVE-2022-45693 :

https://nvd.nist.gov/vuln/detail/cve-2022-45693

- CVE-2023-1436 :

https://nvd.nist.gov/vuln/detail/cve-2023-1436

- CVE-2023-27349 :

https://nvd.nist.gov/vuln/detail/CVE-2023-27349

- CVE-2023-29162 :

https://nvd.nist.gov/vuln/detail/cve-2023-29162

- CVE-2023-39017 :

https://nvd.nist.gov/vuln/detail/cve-2023-39017

- CVE-2023-42917 :

https://nvd.nist.gov/vuln/detail/cve-2023-42917

- CVE-2023-44483 :

https://nvd.nist.gov/vuln/detail/cve-2023-44483

- CVE-2023-49582 :

https://nvd.nist.gov/vuln/detail/cve-2023-49582

- CVE-2023-51074 :

https://nvd.nist.gov/vuln/detail/cve-2023-51074

- CVE-2023-5685 :

https://nvd.nist.gov/vuln/detail/cve-2023-5685

- CVE-2023-7256 :

https://nvd.nist.gov/vuln/detail/cve-2023-7256

- CVE-2024-1135 :

https://nvd.nist.gov/vuln/detail/cve-2024-1135

- CVE-2024-12133 :

https://nvd.nist.gov/vuln/detail/CVE-2024-12133

- CVE-2024-12797 :

https://nvd.nist.gov/vuln/detail/CVE-2024-12797

- CVE-2024-12798 :

https://nvd.nist.gov/vuln/detail/CVE-2024-12798

- CVE-2024-12801 :

https://nvd.nist.gov/vuln/detail/CVE-2024-12801

- CVE-2024-13176 :

https://nvd.nist.gov/vuln/detail/CVE-2024-13176

- CVE-2024-21094 :

https://nvd.nist.gov/vuln/detail/cve-2024-21094

- CVE-2024-21131 :

https://nvd.nist.gov/vuln/detail/cve-2024-21131

- CVE-2024-22201 :

https://nvd.nist.gov/vuln/detail/cve-2024-22201

- CVE-2024-23807 :

https://nvd.nist.gov/vuln/detail/cve-2024-23807

- CVE-2024-24795 :

https://nvd.nist.gov/vuln/detail/cve-2024-24795

- CVE-2024-25638 :

https://nvd.nist.gov/vuln/detail/cve-2024-25638

- CVE-2024-25710 :

https://nvd.nist.gov/vuln/detail/cve-2024-25710

- CVE-2024-26143 :

https://nvd.nist.gov/vuln/detail/CVE-2024-26143

- CVE-2024-26308 :

https://nvd.nist.gov/vuln/detail/cve-2024-26308

- CVE-2024-27309 :

https://nvd.nist.gov/vuln/detail/cve-2024-27309

- CVE-2024-28168 :

https://nvd.nist.gov/vuln/detail/cve-2024-28168

- CVE-2024-28182 :

https://nvd.nist.gov/vuln/detail/cve-2024-28182

- CVE-2024-31141 :

https://nvd.nist.gov/vuln/detail/CVE-2024-31141

- CVE-2024-31744 :

https://nvd.nist.gov/vuln/detail/CVE-2024-31744

- CVE-2024-34064 :

https://nvd.nist.gov/vuln/detail/cve-2024-34064

- CVE-2024-34517 :

https://nvd.nist.gov/vuln/detail/CVE-2024-34517

- CVE-2024-35195 :

https://nvd.nist.gov/vuln/detail/cve-2024-35195

- CVE-2024-37891 :

https://nvd.nist.gov/vuln/detail/cve-2024-37891

- CVE-2024-38356 :

https://nvd.nist.gov/vuln/detail/CVE-2024-38356

- CVE-2024-38357 :

https://nvd.nist.gov/vuln/detail/CVE-2024-38357

- CVE-2024-38472 :

https://nvd.nist.gov/vuln/detail/cve-2024-38472

- CVE-2024-38477 :

https://nvd.nist.gov/vuln/detail/cve-2024-38477

- CVE-2024-38819 :

https://nvd.nist.gov/vuln/detail/cve-2024-38819

- CVE-2024-38820 :

https://nvd.nist.gov/vuln/detail/CVE-2024-38820

- CVE-2024-38827 :

https://nvd.nist.gov/vuln/detail/CVE-2024-38827

- CVE-2024-38828 :

https://nvd.nist.gov/vuln/detail/CVE-2024-38827

- CVE-2024-39884 :

https://nvd.nist.gov/vuln/detail/cve-2024-39884

- CVE-2024-40896 :

https://nvd.nist.gov/vuln/detail/CVE-2024-40896

- CVE-2024-43796 :

https://nvd.nist.gov/vuln/detail/cve-2024-43796

- CVE-2024-45336 :

http://nvd.nist.gov/vuln/detail/cve-2024-45336

- CVE-2024-45340 :

https://nvd.nist.gov/vuln/detail/CVE-2024-45340

- CVE-2024-45341 :

https://nvd.nist.gov/vuln/detail/CVE-2024-45341

- CVE-2024-46956 :

https://nvd.nist.gov/vuln/detail/CVE-2024-46956

- CVE-2024-47072 :

https://nvd.nist.gov/vuln/detail/CVE-2024-47072

- CVE-2024-47554 :

https://nvd.nist.gov/vuln/detail/CVE-2024-47554

- CVE-2024-47561 :

https://nvd.nist.gov/vuln/detail/CVE-2024-47561

- CVE-2024-47606 :

https://nvd.nist.gov/vuln/detail/CVE-2024-47606

- CVE-2024-49767 :

https://nvd.nist.gov/vuln/detail/CVE-2024-49767

- CVE-2024-52012 :

https://nvd.nist.gov/vuln/detail/CVE-2024-52012

- CVE-2024-52046 :

https://nvd.nist.gov/vuln/detail/CVE-2024-52046

- CVE-2024-5535 :

https://nvd.nist.gov/vuln/detail/CVE-2024-5535

- CVE-2024-55549 :

https://nvd.nist.gov/vuln/detail/CVE-2024-55549

- CVE-2024-56128 :

https://nvd.nist.gov/vuln/detail/CVE-2024-56128

- CVE-2024-56171 :

https://nvd.nist.gov/vuln/detail/CVE-2024-56171

- CVE-2024-56201 :

https://nvd.nist.gov/vuln/detail/CVE-2024-56201

- CVE-2024-56326 :

https://nvd.nist.gov/vuln/detail/CVE-2024-56326

- CVE-2024-56406 :

https://nvd.nist.gov/vuln/detail/CVE-2024-56406

- CVE-2024-57699 :

https://nvd.nist.gov/vuln/detail/CVE-2024-57699

- CVE-2024-6763 :

https://nvd.nist.gov/vuln/detail/CVE-2024-6763

- CVE-2024-7254 :

https://nvd.nist.gov/vuln/detail/CVE-2024-7254

- CVE-2024-7264 :

https://nvd.nist.gov/vuln/detail/CVE-2024-7264

- CVE-2024-7592 :

https://nvd.nist.gov/vuln/detail/CVE-2024-7592

- CVE-2024-7885 :

https://nvd.nist.gov/vuln/detail/CVE-2024-7885

- CVE-2024-8006 :

https://nvd.nist.gov/vuln/detail/CVE-2024-8006

- CVE-2024-8176 :

https://nvd.nist.gov/vuln/detail/CVE-2024-8176

- CVE-2024-8184 :

https://nvd.nist.gov/vuln/detail/CVE-2024-8184

- CVE-2024-9143 :

https://nvd.nist.gov/vuln/detail/CVE-2024-9143

- CVE-2024-9287 :

https://nvd.nist.gov/vuln/detail/CVE-2024-9287

- CVE-2025-0395 :

https://nvd.nist.gov/vuln/detail/CVE-2025-0395

- CVE-2025-0624 :

https://nvd.nist.gov/vuln/detail/CVE-2025-0624

- CVE-2025-0725 :

https://nvd.nist.gov/vuln/detail/CVE-2025-0725

- CVE-2025-1948 :

https://nvd.nist.gov/vuln/detail/CVE-2025-1948

- CVE-2025-1974 :

https://nvd.nist.gov/vuln/detail/CVE-2025-1974

- CVE-2025-22228 :

https://nvd.nist.gov/vuln/detail/CVE-2025-22228

- CVE-2025-22865 :

https://nvd.nist.gov/vuln/detail/CVE-2025-22865

- CVE-2025-23016 :

https://nvd.nist.gov/vuln/detail/CVE-2025-23016

- CVE-2025-23083 :

https://nvd.nist.gov/vuln/detail/CVE-2025-23083

- CVE-2025-23084 :

https://nvd.nist.gov/vuln/detail/CVE-2025-23084

- CVE-2025-23085 :

https://nvd.nist.gov/vuln/detail/CVE-2025-23085

- CVE-2025-23165 :

https://nvd.nist.gov/vuln/detail/CVE-2025-23165

- CVE-2025-23166 :

https://nvd.nist.gov/vuln/detail/CVE-2025-23166

- CVE-2025-23167 :

https://nvd.nist.gov/vuln/detail/CVE-2025-23167

- CVE-2025-23184 :

https://nvd.nist.gov/vuln/detail/CVE-2025-23184

- CVE-2025-24813 :

https://nvd.nist.gov/vuln/detail/CVE-2025-24813

- CVE-2025-24814 :

https://nvd.nist.gov/vuln/detail/CVE-2025-24814

- CVE-2025-24855 :

https://nvd.nist.gov/vuln/detail/CVE-2025-24855

- CVE-2025-24928 :

https://nvd.nist.gov/vuln/detail/CVE-2025-24928

- CVE-2025-24970 :

https://nvd.nist.gov/vuln/detail/CVE-2025-24970

- CVE-2025-25193 :

https://nvd.nist.gov/vuln/detail/CVE-2025-25193

- CVE-2025-26791 :

https://nvd.nist.gov/vuln/detail/CVE-2025-26791

- CVE-2025-27113 :

https://nvd.nist.gov/vuln/detail/CVE-2025-27113

- CVE-2025-27363 :

https://nvd.nist.gov/vuln/detail/CVE-2025-27363

- CVE-2025-27516 :

https://nvd.nist.gov/vuln/detail/CVE-2025-27516

- CVE-2025-27533 :

https://nvd.nist.gov/vuln/detail/CVE-2025-27533

- CVE-2025-27636 :

https://nvd.nist.gov/vuln/detail/CVE-2025-27636

- CVE-2025-27817 :

https://nvd.nist.gov/vuln/detail/CVE-2025-27817

- CVE-2025-27818 :

https://nvd.nist.gov/vuln/detail/CVE-2025-27818

- CVE-2025-27819 :

https://nvd.nist.gov/vuln/detail/CVE-2025-27819

- CVE-2025-27820 :

https://nvd.nist.gov/vuln/detail/CVE-2025-27820

- CVE-2025-29482 :

https://nvd.nist.gov/vuln/detail/CVE-2025-29482

- CVE-2025-29891 :

https://nvd.nist.gov/vuln/detail/CVE-2025-29891

- CVE-2025-30065 :

https://nvd.nist.gov/vuln/detail/CVE-2025-30065

- CVE-2025-30474 :

https://nvd.nist.gov/vuln/detail/CVE-2025-30474

- CVE-2025-30739 :

https://nvd.nist.gov/vuln/detail/CVE-2025-30739

- CVE-2025-30743 :

https://nvd.nist.gov/vuln/detail/CVE-2025-30743

- CVE-2025-30744 :

https://nvd.nist.gov/vuln/detail/CVE-2025-30744

- CVE-2025-30745 :

https://nvd.nist.gov/vuln/detail/CVE-2025-30745

- CVE-2025-30746 :

https://nvd.nist.gov/vuln/detail/CVE-2025-30746

- CVE-2025-30747 :

https://nvd.nist.gov/vuln/detail/CVE-2025-30747

- CVE-2025-30748 :

https://nvd.nist.gov/vuln/detail/CVE-2025-30748

- CVE-2025-30749 :

https://nvd.nist.gov/vuln/detail/CVE-2025-30749

- CVE-2025-30750 :

https://nvd.nist.gov/vuln/detail/CVE-2025-30750

- CVE-2025-30751 :

https://nvd.nist.gov/vuln/detail/CVE-2025-30751

- CVE-2025-30752 :

https://nvd.nist.gov/vuln/detail/CVE-2025-30752

- CVE-2025-30753 :

https://nvd.nist.gov/vuln/detail/CVE-2025-30753

- CVE-2025-30754 :

https://nvd.nist.gov/vuln/detail/CVE-2025-30754

- CVE-2025-30756 :

https://nvd.nist.gov/vuln/detail/CVE-2025-30756

- CVE-2025-30758 :

https://nvd.nist.gov/vuln/detail/CVE-2025-30758

- CVE-2025-30759 :

https://nvd.nist.gov/vuln/detail/CVE-2025-30759

- CVE-2025-30760 :

https://nvd.nist.gov/vuln/detail/CVE-2025-30760

- CVE-2025-30761 :

https://nvd.nist.gov/vuln/detail/CVE-2025-30761

- CVE-2025-30762 :

https://nvd.nist.gov/vuln/detail/CVE-2025-30762

- CVE-2025-31650 :

https://nvd.nist.gov/vuln/detail/CVE-2025-31650

- CVE-2025-31651 :

https://nvd.nist.gov/vuln/detail/CVE-2025-31651

- CVE-2025-31672 :

https://nvd.nist.gov/vuln/detail/CVE-2025-31672

- CVE-2025-31720 :

https://nvd.nist.gov/vuln/detail/CVE-2025-31720

- CVE-2025-31721 :

https://nvd.nist.gov/vuln/detail/CVE-2025-31721

- CVE-2025-32414 :

https://nvd.nist.gov/vuln/detail/CVE-2025-32414

- CVE-2025-32415 :

https://nvd.nist.gov/vuln/detail/CVE-2025-32415

- CVE-2025-4598 :

https://nvd.nist.gov/vuln/detail/CVE-2025-4598

- CVE-2025-46701 :

https://nvd.nist.gov/vuln/detail/CVE-2025-46701

- CVE-2025-47287 :

https://nvd.nist.gov/vuln/detail/CVE-2025-47287

- CVE-2025-4802 :

https://nvd.nist.gov/vuln/detail/CVE-2025-4802

- CVE-2025-48734 :

https://nvd.nist.gov/vuln/detail/CVE-2025-48734

- CVE-2025-48976 :

https://nvd.nist.gov/vuln/detail/CVE-2025-48976

- CVE-2025-48988 :

https://nvd.nist.gov/vuln/detail/CVE-2025-48988

- CVE-2025-49124 :

https://nvd.nist.gov/vuln/detail/CVE-2025-49124

- CVE-2025-49125 :

https://nvd.nist.gov/vuln/detail/CVE-2025-49125

- CVE-2025-49146 :

https://nvd.nist.gov/vuln/detail/CVE-2025-49146

- CVE-2025-50059 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50059

- CVE-2025-50060 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50060

- CVE-2025-50061 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50061

- CVE-2025-50062 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50062

- CVE-2025-50063 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50063

- CVE-2025-50064 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50064

- CVE-2025-50065 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50065

- CVE-2025-50066 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50066

- CVE-2025-50067 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50067

- CVE-2025-50068 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50068

- CVE-2025-50069 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50069

- CVE-2025-50070 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50070

- CVE-2025-50071 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50071

- CVE-2025-50072 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50072

- CVE-2025-50073 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50073

- CVE-2025-50076 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50076

- CVE-2025-50077 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50077

- CVE-2025-50078 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50078

- CVE-2025-50079 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50079

- CVE-2025-50080 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50080

- CVE-2025-50081 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50081

- CVE-2025-50082 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50082

- CVE-2025-50083 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50083

- CVE-2025-50084 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50084

- CVE-2025-50085 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50085

- CVE-2025-50086 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50086

- CVE-2025-50087 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50087

- CVE-2025-50088 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50088

- CVE-2025-50089 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50089

- CVE-2025-50090 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50090

- CVE-2025-50091 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50091

- CVE-2025-50092 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50092

- CVE-2025-50093 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50093

- CVE-2025-50094 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50094

- CVE-2025-50095 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50095

- CVE-2025-50096 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50096

- CVE-2025-50097 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50097

- CVE-2025-50098 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50098

- CVE-2025-50099 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50099

- CVE-2025-50100 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50100

- CVE-2025-50101 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50101

- CVE-2025-50102 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50102

- CVE-2025-50103 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50103

- CVE-2025-50104 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50104

- CVE-2025-50105 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50105

- CVE-2025-50106 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50106

- CVE-2025-50107 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50107

- CVE-2025-50108 :

https://nvd.nist.gov/vuln/detail/CVE-2025-50108

- CVE-2025-53023 :

https://nvd.nist.gov/vuln/detail/CVE-2025-53023

- CVE-2025-53024 :

https://nvd.nist.gov/vuln/detail/CVE-2025-53024

- CVE-2025-53025 :

https://nvd.nist.gov/vuln/detail/CVE-2025-53025

- CVE-2025-53026 :

https://nvd.nist.gov/vuln/detail/CVE-2025-53026

- CVE-2025-53027 :

https://nvd.nist.gov/vuln/detail/CVE-2025-53027

- CVE-2025-53028 :

https://nvd.nist.gov/vuln/detail/CVE-2025-53028

- CVE-2025-53029 :

https://nvd.nist.gov/vuln/detail/CVE-2025-53029

- CVE-2025-53030 :

https://nvd.nist.gov/vuln/detail/CVE-2025-53030

- CVE-2025-53031 :

https://nvd.nist.gov/vuln/detail/CVE-2025-53031

- CVE-2025-53032 :

https://nvd.nist.gov/vuln/detail/CVE-2025-53032

- CVE-2025-5399 :

https://nvd.nist.gov/vuln/detail/CVE-2025-5399