Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0328

Kwetsbaarheden verholpen in Oracle Database producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 23-10-2025

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Oracle heeft kwetsbaarheden verholpen in Oracle Database Server producten

Duiding

De kwetsbaarheden in Oracle Database Server stellen ongeauthenticeerde aanvallers in staat om ongeoorloofde toegang te verkrijgen tot kritieke gegevens, wat kan leiden tot schending van de vertrouwelijkheid, integriteit en beschikbaarheid van de data. Specifieke kwetsbaarheden, zoals die in de Portable Clusterware en de Unified Audit componenten, kunnen worden misbruikt door aanvallers met beperkte privileges, wat aanzienlijke risico's met zich meebrengt. De CVSS-scores variëren van 2.7 tot 9.8, afhankelijk van de ernst van de kwetsbaarheid.

Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.oracle.com/docs/tech/security-alerts/cpuoct2025csaf.json

Kwetsbaarheden

CVE	CVSS Score
CVE-2020-13956	5.3 MEDIUM
CVE-2024-52577	9.5 CRITICAL
CVE-2024-57699	5.1 MEDIUM
CVE-2025-4517	6.9 MEDIUM
CVE-2025-4949	6.8 MEDIUM
CVE-2025-8885	6.3 MEDIUM
CVE-2025-8916	6.3 MEDIUM
CVE-2025-48976	8.7 HIGH

CVE-2025-52520	6.3 MEDIUM
CVE-2025-53047	5.8 MEDIUM
CVE-2025-53051	2.7 LOW
CVE-2025-53864	6.9 MEDIUM
CVE-2025-61749	2.7 LOW
CVE-2025-61763	8.1 HIGH
CVE-2025-61881	5.9 MEDIUM

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-125	Out-of-bounds Read
CWE-190	Integer Overflow or Wraparound
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-284	Improper Access Control
CWE-404	Improper Resource Shutdown or Release
CWE-502	Deserialization of Untrusted Data
CWE-611	Improper Restriction of XML External Entity Reference
CWE-674	Uncontrolled Recursion
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-827	Improper Control of Document Type Definition
CWE-937	CWE-937

CWE-1035	CWE-1035

Getroffen producten

Oracle
Clusterware
Database Server
Essbase
Essbase Server
GoldenGate Big Data and Application Adapters
GoldenGate Stream Analytics
GoldenGate for Big Data
Goldengate Application Adapters
Goldengate Big Data
Goldengate Veridata
Graph Server And Client
Java Virtual Machine
REST Data Services
SQLcl

Disclaimer