



# 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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto: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
➤ <a href="#">CVE-2020-13956</a>	5.3 MEDIUM
➤ <a href="#">CVE-2024-52577</a>	9.5 CRITICAL
➤ <a href="#">CVE-2024-57699</a>	5.1 MEDIUM
➤ <a href="#">CVE-2025-4517</a>	6.9 MEDIUM
➤ <a href="#">CVE-2025-4949</a>	6.8 MEDIUM
➤ <a href="#">CVE-2025-8885</a>	6.3 MEDIUM
➤ <a href="#">CVE-2025-8916</a>	6.3 MEDIUM
➤ <a href="#">CVE-2025-48976</a>	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
> CVE-20	Improper Input Validation
> CVE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
> CVE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
> CVE-125	Out-of-bounds Read
> CVE-190	Integer Overflow or Wraparound
> CVE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CVE-284	Improper Access Control
> CVE-404	Improper Resource Shutdown or Release
> CVE-502	Deserialization of Untrusted Data
> CVE-611	Improper Restriction of XML External Entity Reference
> CVE-674	Uncontrolled Recursion
> CVE-770	Allocation of Resources Without Limits or Throttling
> CVE-827	Improper Control of Document Type Definition
> CVE-937	CWE-937

[> CWE-1035](#)

CWE-1035

## Getroffen producten

<b>Oracle</b>
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

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.