



NCSC-2026-0021

Kwetsbaarheden verholpen in Oracle Database Server producten

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 21-01-2026

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 niet-geauthenticeerde aanvallers in staat om de integriteit en vertrouwelijkheid van gegevens te compromitteren. Dit kan leiden tot ongeautoriseerde toegang tot gevoelige data en zelfs een mogelijke overname van de SQLcl-component.

Oplossingen

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

Referenties

➤ <https://www.oracle.com/security-alerts/cpujan2026.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-8194	7.5 HIGH
➤ CVE-2025-12383	9.4 CRITICAL
➤ CVE-2025-30065	10.0 CRITICAL
➤ CVE-2025-48924	6.5 MEDIUM
➤ CVE-2025-54874	6.6 MEDIUM
➤ CVE-2025-55039	6.3 MEDIUM
➤ CVE-2025-59250	8.1 HIGH
➤ CVE-2025-59419	7.7 HIGH
➤ CVE-2025-61755	3.7 LOW

> CVE-2025-61795	2.3 LOW
> CVE-2025-65082	5.1 MEDIUM
> CVE-2025-66566	8.2 HIGH
> CVE-2025-67735	6.9 MEDIUM
> CVE-2025-68161	6.3 MEDIUM
> CVE-2026-21931	5.4 MEDIUM
> CVE-2026-21939	7.3 HIGH
> CVE-2026-21975	4.5 MEDIUM
> CVE-2026-21977	2.3 LOW

CWE's

CWE	Beschrijving
> CWE-20	Improper Input Validation
> CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
> CWE-93	Improper Neutralization of CRLF Sequences ('CRLF Injection')
> CWE-150	Improper Neutralization of Escape, Meta, or Control Sequences
> CWE-201	Insertion of Sensitive Information Into Sent Data
> CWE-295	Improper Certificate Validation
> CWE-297	Improper Validation of Certificate with Host Mismatch
> CWE-326	Inadequate Encryption Strength
> CWE-347	Improper Verification of Cryptographic Signature
> CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
> CWE-404	Improper Resource Shutdown or Release
> CWE-457	Use of Uninitialized Variable

> CWE-502	Deserialization of Untrusted Data
> CWE-674	Uncontrolled Recursion
> CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')
> CWE-862	Missing Authorization
> CWE-908	Use of Uninitialized Resource
> CWE-937	CWE-937
> CWE-1035	CWE-1035

Getroffen producten

Oracle
Core RDBMS
Essbase
Fleet Patching and Provisioning
GoldenGate
GoldenGate Big Data and Application Adapters
Goldengate Stream Analytics
GraalVM
Graph Server And Client
Java Virtual Machine
NoSQL Database
Oracle APEX Sample Applications

Oracle Database Server
Oracle Graal Development Kit for Micronaut
Oracle Zero Data Loss Recovery Appliance Software
SQLcl
Secure Backup
Spatial and Graph

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.