



NCSC-2026-0307

Kwetsbaarheden verholpen in Oracle Database Producten

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 19-08-2026

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 diverse Database producten als de Database Server, Essbase, Autonomous Health Framework en de Application Testing Suite

Duiding

Oracle Database Server (versies 19.3 tot 23.26.3) bevat kritieke kwetsbaarheden in de RDBMS en Portable Clusterware componenten, waaronder mogelijkheden voor ongeauthenticeerde aanvallers met fysieke of netwerktoegang om controle te verkrijgen over clusterware, volledige controle over de RDBMS te verkrijgen, of ongeautoriseerde lees- en schrijfbewerkingen uit te voeren. Sommige kwetsbaarheden vereisen fysieke toegang tot communicatie segmenten, andere kunnen via netwerktoegang worden misbruikt.

Oracle Essbase kent kwetsbaarheden die een aanvaller met netwerktoegang via HTTP in staat stellen volledige systeemcompromittatie te bereiken.

Oracle Autonomous Health Framework bevat meerdere kwetsbaarheden in de Trace File Analyzer en Cluster Health Analyzer componenten, die ongeautoriseerde toegang, datamanipulatie en denial of service mogelijk maken, afhankelijk van privileges en netwerktoegang.

Oracle Application Testing Suite versie 13.3.0.1 bevat diverse kwetsbaarheden die ongeauthenticeerde of laaggeprivilegieerde aanvallers met netwerktoegang via HTTP(S) in staat stellen kritieke data te creëren, wijzigen of verwijderen, privileges te escaleren en volledige systeemcompromis te bereiken.

Deze kwetsbaarheden kunnen leiden tot datalekken, datamanipulatie, denial of service en volledige systeemcompromittatie.

Oplossingen

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

Referenties

➤ <https://www.oracle.com/security-alerts/cspuag2026.html>

Kwetsbaarheden

CVE	CVSS Score

> CVE-2026-9563	7.5 HIGH
> CVE-2026-29167	9.8 CRITICAL
> CVE-2026-42764	7.5 HIGH
> CVE-2026-45447	8.8 HIGH
> CVE-2026-59889	6.5 MEDIUM
> CVE-2026-70688	8.8 HIGH
> CVE-2026-70689	9.8 CRITICAL
> CVE-2026-70715	8.8 HIGH
> CVE-2026-70717	7.7 HIGH
> CVE-2026-70728	8.5 HIGH
> CVE-2026-70731	8.4 HIGH
> CVE-2026-70734	7.4 HIGH
> CVE-2026-70862	9.1 CRITICAL
> CVE-2026-70863	8.8 HIGH
> CVE-2026-70864	7.6 HIGH
> CVE-2026-70865	7.5 HIGH
> CVE-2026-70866	7.8 HIGH
> CVE-2026-70867	7.1 HIGH
> CVE-2026-70868	8.1 HIGH
> CVE-2026-71062	8.5 HIGH
> CVE-2026-71063	9.6 CRITICAL
> CVE-2026-71064	9.6 CRITICAL
> CVE-2026-71100	5.3 MEDIUM

> [CVE-2026-71102](#)

9.1 CRITICAL

CWE's

CWE	Beschrijving
> CWE-400	Uncontrolled Resource Consumption
> CWE-416	Use After Free
> CWE-476	NULL Pointer Dereference
> CWE-502	Deserialization of Untrusted Data
> CWE-770	Allocation of Resources Without Limits or Throttling
> CWE-825	Expired Pointer Dereference
> CWE-863	Incorrect Authorization

Getroffen producten

Oracle

Database
Server

Oracle Corporation

Oracle Application
Testing Suite

Oracle Autonomous Health
Framework

Oracle
Essbase

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.