Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0373

Kwetsbaarheden verholpen in Oracle Database Producten

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 16-09-2026

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 16 kwetsbaarheden verholpen in diverse Database producten, waaronder Database Server, Autonomous Health Framework en Application Testing Suite.

Duiding

De kwetsbaarheden betreffen verschillende beveiligingsproblemen in Oracle-producten, waaronder mogelijkheden voor niet-geauthenticeerde en laaggeprivilegieerde kwaadwillenden om via netwerktoegang ongeautoriseerde acties uit te voeren. De kwetsbaarheden hebben CVSS-scores variërend van middel tot kritiek. Van de in totaal 16 kwetsbaarheden is één als kritiek aangemerkt en kunnen zes zonder authenticatie op afstand worden misbruikt. Succesvol misbruik kan onder meer leiden tot ongeautoriseerde toegang tot gevoelige informatie, het wijzigen van gegevens en het verstoren van de beschikbaarheid van getroffen systemen. Sommige kwetsbaarheden vereisen gebruikersinteractie of voorafgaande toegangsrechten, terwijl andere volledig op afstand en zonder authenticatie kunnen worden misbruikt.

De kritieke kwetsbaarheid, CVE-2026-83149, heeft een CVSS-score van 9,1 en bevindt zich in Test Manager for Web Apps van Oracle Application Testing Suite. Volgens Oracle is een laaggeprivilegieerd account voor misbruik vereist en is geen gebruikersinteractie nodig. Succesvolle exploitatie kan een hoge impact hebben op de vertrouwelijkheid en een beperkte impact op de integriteit en beschikbaarheid van het getroffen systeem.

Het NCSC adviseert om de beveiligingsupdate voor de kritieke kwetsbaarheid met voorrang toe te passen.

Oplossingen

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

Referenties

- https://www.oracle.com/security-alerts/cspusep2026.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-14456	7.5 HIGH
CVE-2026-75838	5.1 MEDIUM

CVE-2026-83088	7.7 HIGH
CVE-2026-83148	8.8 HIGH
CVE-2026-83149	9.1 CRITICAL
CVE-2026-83150	7.0 HIGH
CVE-2026-83156	7.5 HIGH
CVE-2026-83160	8.8 HIGH
CVE-2026-83271	8.8 HIGH
CVE-2026-83272	8.5 HIGH
CVE-2026-83333	7.5 HIGH
CVE-2026-83347	6.5 MEDIUM
CVE-2026-83348	8.8 HIGH
CVE-2026-83349	7.5 HIGH
CVE-2026-83350	7.5 HIGH
CVE-2026-83351	8.1 HIGH

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-770	Allocation of Resources Without Limits or Throttling

Getroffen producten

Oracle
Database Server

Oracle Application
Testing Suite

Oracle Autonomous Health
Framework

Oracle Database
Server

Oracle Corporation

Oracle Application
Testing Suite

Disclaimer