Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0169

Kwetsbaarheden verholpen in Oracle Database Server

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 29-05-2026

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 REST Data Services (versies 24.2.0 tot 26.1.0) en Oracle Database Server (versies 23.4.0 tot 23.26.2).

Duiding

De kwetsbaarheden in Oracle REST Data Services stellen een aanvaller met lage privileges en netwerktoegang via HTTPS in staat om zonder authenticatie verschillende acties uit te voeren, waaronder het volledig overnemen van de service, ongeautoriseerde toegang tot data, het wijzigen of verwijderen van data, en het veroorzaken van een denial-of-service. Sommige kwetsbaarheden maken het mogelijk om authenticatie te omzeilen en willekeurige acties uit te voeren binnen de getroffen omgeving. Daarnaast kunnen denial-of-service-condities worden veroorzaakt door het laten hangen of crashen van de service. In Oracle Database Server kunnen ongeauthenticeerde aanvallers met netwerktoegang via TLS de Net Service-component overnemen of een denial-of-service veroorzaken, wat impact heeft op vertrouwelijkheid, integriteit en beschikbaarheid. Verder is er een kwetsbaarheid in Eclipse Jetty's HTTP/1.1 parser die request smuggling mogelijk maakt door onjuiste verwerking van chunked transfer encoding extensions, wat kan leiden tot beveiligingsomzeilingen zoals cache poisoning en sessiekaping. Voor deze Jetty-kwetsbaarheid zijn momenteel geen patches of mitigaties beschikbaar.

Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden in Oracle REST Data Services en Oracle Database Server te verhelpen. Voor de kwetsbaarheid in Eclipse Jetty's HTTP/1.1 parser zijn op dit moment geen patches of mitigaties beschikbaar. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.oracle.com/security-alerts/cspumay2026.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-2332	2.3 LOW
CVE-2026-35266	7.9 HIGH
CVE-2026-35277	8.1 HIGH

CVE-2026-46775	9.9 CRITICAL
CVE-2026-46829	7.5 HIGH
CVE-2026-46830	5.3 MEDIUM
CVE-2026-46833	9.0 CRITICAL
CVE-2026-46834	7.5 HIGH
CVE-2026-46835	7.5 HIGH
CVE-2026-46839	9.9 CRITICAL
CVE-2026-46840	10.0 CRITICAL
CVE-2026-46841	5.3 MEDIUM
CVE-2026-46842	5.3 MEDIUM
CVE-2026-46843	5.3 MEDIUM

CWE's

CWE	Beschrijving
CWE-269	Improper Privilege Management
CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
CWE-937	OWASP Top Ten 2013 Category A9 - Using Components with Known Vulnerabilities
CWE-1035	OWASP Top Ten 2017 Category A9 - Using Components with Known Vulnerabilities

Getroffen producten

Oracle
Database Server

REST Data
Services

Disclaimer