Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0254

Kwetsbaarheden verholpen in Oracle database producten

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 22-07-2026

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 158 kwetsbaarheden verholpen in Oracle Database Server, APEX, Autonomous Health Framework, Essbase, Global Lifecycle Management, GoldenGate, NoSQL Database, Spatial Studio, SQL Developer en TimesTen In-Memory Database.

Van deze kwetsbaarheden zijn 91 kwetsbaarheden afkomstig van third-party producten waarvoor eerder al updates zijn verschenen welke nu door Oracle zijn verwerkt, of betreffen kwetsbaarheden welke niet kunnen leiden tot exploitatie, omdat zij zich bevinden in delen van de producten die niet toegankelijk zijn.

Duiding

De zes ernstigste kwetsbaarheden hebben een CVSS score van 9 en hoger gekregen.

De kwetsbaarheid in Eclipse Jetty's HTTP/1.1 parser, gebruikt in Oracle REST Data Services versies 24.2.0 tot 26.1.0, betreft incorrecte parsing van chunked transfer encoding extensies met ongesloten gequoteerde strings, waardoor HTTP request smuggling mogelijk is. Dit kan leiden tot cache poisoning, bypass van toegangscontrole, session hijacking en ongeautoriseerde toegang tot endpoints.

Perl versies vanaf 5.9.4 tot 5.43.9 bevatten een kwetsbare Compress::Raw::Zlib module door een verouderde zlib bibliotheek met meerdere beveiligingsproblemen, waaronder CVE-2026-3381 en CVE-2026-27171. Deze kwetsbaarheid is relevant voor Perl distributies die vaak worden ingezet in Red Hat Enterprise Linux en OpenShift Container Platform omgevingen.

Apache Kafka versies 4.1.0 en 4.1.1 bevatten een kwetsbaarheid in de JWT token validatie waarbij de standaard validator elke JWT token accepteert zonder correcte validatie, wat ongeautoriseerde toegang kan toestaan. Dit is opgelost door de validator expliciet in te stellen of te upgraden naar versie 4.1.2 of hoger. Oracle Communications Unified Assurance Message Bus componenten versies 6.1.1 tot 7.0.0, die Apache Kafka gebruiken, bevatten een kwetsbaarheid die ongeauthenticeerde netwerkaanvallers in staat stelt ongeautoriseerde toegang te verkrijgen en kritieke data te wijzigen.

Oracle Net Services versies 19.3 tot 19.31, 21.3 tot 21.22 en 23.4.0 tot 23.26.2 bevatten een kwetsbaarheid die ongeauthenticeerde netwerktoegang mogelijk maakt om gevoelige informatie te verkrijgen of een denial of service te veroorzaken.

Oracle TimesTen In-Memory Database versie 26.1.1.1.0 bevat een kwetsbaarheid in de Kubernetes Operator component die een aanvaller met lage privileges en netwerktoegang via HTTPS in staat stelt volledige controle over de database instance te verkrijgen.

Oracle Database Server RDBMS componenten versies 19.3 tot 19.31 en 23.4.0 tot 23.26.2 bevatten een kwetsbaarheid waarbij een aanvaller met lage privileges en Execute DBMS_CLOUD rechten en netwerktoegang volledige controle over de RDBMS kan verkrijgen.

Het voert te ver om de overige 152 kwetsbaarheden in detail te beschrijven in deze advisory en het NCSC verwijst dan ook naar de bijgevoegde referentie.

Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Voor Apache Kafka wordt aanbevolen te upgraden naar versie 4.1.2 of hoger en de JWT validator expliciet in te stellen. Voor Perl is een update van de Compress::Raw::Zlib module beschikbaar in de nieuwste versies. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.oracle.com/security-alerts/cpujul2026.html
- https://www.oracle.com/security-alerts/cpujul2026verbose.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-2332	2.3 LOW
CVE-2026-4176	9.8 CRITICAL
CVE-2026-33557	6.3 MEDIUM
CVE-2026-47040	9.1 CRITICAL
CVE-2026-60402	9.9 CRITICAL
CVE-2026-61211	9.9 CRITICAL

CWE's

CWE	Beschrijving
CWE-287	Improper Authentication
CWE-303	Incorrect Implementation of Authentication Algorithm
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
CWE-1104	Use of Unmaintained Third Party Components
CWE-1285	Improper Validation of Specified Index, Position, or Offset in Input
CWE-1395	Dependency on Vulnerable Third-Party Component

Getroffen producten

Oracle
APEX
Autonomous Health Framework
Essbase
Global Lifecycle Management
GoldenGate
NoSQL Database
Oracle Database Server
Oracle REST Data Services
SQL Developer
Spatial Studio

Oracle Corporation
Oracle Net Services
TimesTen In-Memory Database

Disclaimer