Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0256

Kwetsbaarheden verholpen in Oracle Communications

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 kwetsbaarheden verholpen in Communications producten en onderliggende third party software. Het betreft een totaal van 213 kwetsbaarheden, waarvan 67 zich bevinden in Oracle producten en 146 in third-party producten waar eerder updates voor zijn verschenen en welke in deze Oracle updates zijn verwerkt.

Duiding

De ernstigste kwetsbaarheden, 12 stuks, hebben een CVSS score van 9 en hoger gekregen en zijn hieronder omschreven. 11 hiervan bevinden zich in embedded third-party producten.

De overige kwetsbaarheden hebben lagere scores gekregen en het voert te ver om detailinformatie op te nemen in deze advisory. Hiervoor verwijst het NCSC naar de bijgevoegde referentie.

Oracle Communications Converged Application Server versies 8.2 en 8.3 bevatten een kwetsbaarheid die onbevoegde netwerktoegang mogelijk maakt en kan leiden tot volledige overname van het systeem.

Libtiff tot versie 4.7.0 bevat een write-what-where kwetsbaarheid en een stack-based buffer overflow die kunnen worden geactiveerd door speciaal vervaardigde TIFF-bestanden, wat kan leiden tot code-executie of crashes.

Apache Tomcat versies 8.5.0 tot 11.0.5 bevatten kwetsbaarheden waardoor speciaal opgemaakte HTTP-verzoeken rewrite rules en security constraints kunnen omzeilen, met mogelijke data disclosure, wijziging of denial of service als gevolg.

Eclipse Jetty's HTTP/1.1 parser verwerkt chunked transfer encoding extensies met onjuist gesloten aanhalingstekens verkeerd, wat request smuggling mogelijk maakt en kan leiden tot cache poisoning, access control bypass en sessie kaping.

Perl versies met een verouderde vendored zlib in Compress::Raw::Zlib bevatten meerdere beveiligingsproblemen die zijn opgelost in een specifieke commit.

Lodash versies tot 4.17.23 bevatten meerdere kwetsbaarheden waaronder code-injectie via onbetrouwbare keys in _.template, prototype pollution, regex denial of service en command injection.

Apache HTTP Server versies 2.4.0 tot 2.4.67 bevatten diverse kwetsbaarheden in meerdere modules die kunnen leiden tot server crashes, code-executie, cross-site scripting en informatielekken.

Apache Kafka versies 4.1.0 en 4.1.1 hebben een kwetsbaarheid in de JWT token validatie waardoor onbevoegde toegang mogelijk is.

AIOHTTP versies voor 3.13.4 accepteren null bytes en control characters in HTTP headers, wat header injectie en response splitting mogelijk maakt.

De cryptography package van versies 45.0.0 tot 46.0.7 bevat een buffer overflow bij het verwerken van niet-contigu buffers op Python 3.11+, wat kan leiden tot crashes of informatielekken.

Spring Boot versies 4.0.0 tot 4.0.5 bevatten een kwetsbaarheid die het mogelijk maakt om de standaard web security te omzeilen.

Apache MINA versies 2.1.X en 2.2.X bevatten meerdere deserialisatie kwetsbaarheden die code-executie mogelijk maken door bypass van classname allowlist en filters.

Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Gebruikers wordt geadviseerd de relevante updates te installeren. 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-2025-9900	5.3 MEDIUM
CVE-2025-31651	2.7 LOW
CVE-2026-2332	2.3 LOW
CVE-2026-4176	9.8 CRITICAL
CVE-2026-4800	9.8 CRITICAL
CVE-2026-29167	6.9 MEDIUM
CVE-2026-33557	6.3 MEDIUM
CVE-2026-34520	2.7 LOW
CVE-2026-39892	6.9 MEDIUM
CVE-2026-40976	6.9 MEDIUM

CVE-2026-42779	**6.9 MEDIUM**
CVE-2026-61223	**9.0 CRITICAL**

CWE's

CWE	Beschrijving
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor

Getroffen producten

Oracle
Communications Element Manager
Oracle Communications
Oracle Communications Cloud Native Core Network Repository Function
Oracle Communications Cloud Native Core Network Slice Selection Function
Oracle Communications Cloud Native Core Service Communication Proxy
Oracle Communications Policy Management
Oracle Communications Session Report Manager
Oracle Communications Unified Assurance
Oracle Corporation
Oracle Communications Converged Application Server

Disclaimer