



NCSC-2026-0200

Kwetsbaarheden verholpen in Oracle Communications

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 17-06-2026

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 Communications

Duiding

De kwetsbaarheden zitten in twee onderliggende producten: SQLite en Log4j en zijn eerder verholpen door de ontwikkelaars van deze producten. Oracle heeft de updates verwerkt in de eigen software. In SQLite kan een remote aanvaller via speciaal vervaardigde ZIP-bestanden heap geheugen uitlekken door een informatielek in de zipfileInflate functie van de zipfile extensie. In Log4j leidt onjuiste serialisatie van niet-eindige floating-point waarden zoals NaN of infinity in de JsonTemplateLayout tot ongeldig JSON-output, wat downstream logverwerkende systemen kan verstoren. Dit kan misbruikt worden als applicaties door de aanvaller gecontroleerde MapMessages loggen, wat een denial of service in loganalyse workflows veroorzaakt.

Oplossingen

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

Referenties

➤ <https://www.oracle.com/security-alerts/cspujun2026.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-70873	7.5 HIGH
➤ CVE-2026-34481	6.3 MEDIUM

CWE's

CWE	Beschrijving
➤ CWE-116	Improper Encoding or Escaping of Output
➤ CWE-241	Improper Handling of Unexpected Data Type
➤ CWE-244	Improper Clearing of Heap Memory Before Release ('Heap Inspection')

> [CWE-908](#)

Use of Uninitialized Resource

Getroffen producten

Oracle

Oracle Communications Convergent
Charging Controller

Oracle Communications Network
Charging and Control

Oracle Communications
Network Integrity

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.