



Advisory NCSC-2026-0444

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Oracle Communications

Publicatiedatum: 21-10-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Oracle heeft 110 kwetsbaarheden verholpen in diverse Oracle Communications-producten, waaronder Oracle Communications Unified Assurance, Oracle Communications Cloud Native Core Security Edge Protection Proxy, Oracle Communications Service Catalog and Design en Oracle Communications Operations Monitor.

Duiding

De kwetsbaarheden betreffen verschillende beveiligingsproblemen in Oracle Communications-producten, waaronder mogelijkheden voor niet-geauthenticeerde en laaggeprivilegieerde kwaadwillenden om via netwerktoegang ongeautoriseerde acties uit te voeren. De kwetsbaarheden hebben CVSS-scores variërend van laag tot kritiek, met een maximale score van 9,8. De update bevat in totaal 110 kwetsbaarheden voor Oracle Communications, waarvan 77 kwetsbaarheden op afstand zonder authenticatie kunnen worden misbruikt. Succesvol misbruik kan, afhankelijk van de specifieke kwetsbaarheid, leiden tot ongeautoriseerde toegang tot gevoelige informatie, het wijzigen van gegevens of het verstoren van de beschikbaarheid van getroffen systemen. Sommige kwetsbaarheden vereisen voorafgaande toegangsrechten of gebruikersinteractie, terwijl andere via netwerktoegang zonder authenticatie kunnen worden misbruikt.

Oplossingen

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

Referenties

- <https://www.oracle.com/security-alerts/cpuoct2026.html>

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-48734	9.3 CRITICAL
CVE-2026-5450	9.8 CRITICAL
CVE-2026-6653	8.3 HIGH
CVE-2026-8763	9.3 CRITICAL
CVE-2026-10050	8.7 HIGH
CVE-2026-13221	9.1 CRITICAL
CVE-2026-13321	8.6 HIGH
CVE-2026-21716	8.4 HIGH
CVE-2026-28369	9.1 CRITICAL
CVE-2026-29167	9.8 CRITICAL
CVE-2026-32327	9.1 CRITICAL
CVE-2026-39892	6.9 MEDIUM
CVE-2026-41855	8.1 HIGH
CVE-2026-54906	2.1 LOW
CVE-2026-56130	2.0 LOW
CVE-2026-58016	9.1 CRITICAL
CVE-2026-58389	8.7 HIGH
CVE-2026-61674	9.2 CRITICAL
CVE-2026-63388	8.4 HIGH
CVE-2026-63639	8.8 HIGH
CVE-2026-64193	9.8 CRITICAL
CVE-2026-68525	9.1 CRITICAL
CVE-2026-75595	9.1 CRITICAL
CVE-2026-75596	8.7 HIGH
CVE-2026-78030	9.8 CRITICAL
CVE-2026-84939	9.1 CRITICAL
CVE-2026-86219	9.8 CRITICAL
CVE-2026-101758	8.2 HIGH

CVE	CVSS Score
CVE-2026-101763	9.8 CRITICAL
CVE-2026-101765	9.1 CRITICAL
CVE-2026-101791	8.1 HIGH

CWE's

CWE	Beschrijving
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-121	Stack-based Buffer Overflow
CWE-122	Heap-based Buffer Overflow
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-416	Use After Free
CWE-502	Deserialization of Untrusted Data

Getroffen producten

Oracle
Communications
Communications Applications
Communications Billing and Revenue Management
Construction and Engineering

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 or 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.