Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0309

Kwetsbaarheden verholpen in Oracle Communications

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 19-08-2026

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 verschillende Communications-modules, waaronder Oracle Communications Cloud Native Core Network Exposure Function, Oracle Commerce Guided Search en Oracle Communications Unified Inventory Management

Duiding

De kwetsbaarheden betreffen onder andere stack-based buffer overflows, onjuiste validatie van input, prototype pollution, improper authorization, use-after-free, deserialization filter bypass, en onvoldoende toegangscontrole. Aanvallers kunnen deze kwetsbaarheden misbruiken om onder meer Denial of Service (DoS) te veroorzaken, ongeautoriseerde toegang te verkrijgen, gevoelige data te wijzigen of in te zien, arbitrary code execution uit te voeren, en volledige systeemcompromittering te bereiken. Specifiek kunnen sommige kwetsbaarheden leiden tot privilege escalatie, bypass van authenticatie, en remote code execution zonder authenticatie. De kwetsbaarheden zijn aanwezig in diverse versies van de genoemde producten en modules, waarbij sommige fixes reeds zijn uitgebracht in specifieke versies. Controleer daarom of de specifieke kwetsbaarheden van toepassing zijn op het eigen systeem.

Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Het wordt aanbevolen om de meest recente versies van de betreffende producten te installeren, zoals Oracle Communications Cloud Native Core Network Exposure Function versie 24.2.1 en hoger, Oracle Commerce Guided Search 11.4.0 en hoger, en de updates voor Oracle Communications Unified Inventory Management vanaf versie 8.0.2. Daarnaast zijn er patches beschikbaar voor de overige genoemde producten en modules. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.oracle.com/security-alerts/cspuaug2026.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-13151	7.5 HIGH
CVE-2026-4176	9.8 CRITICAL
CVE-2026-4800	9.8 CRITICAL

CVE-2026-5795	7.4 HIGH
CVE-2026-29167	9.8 CRITICAL
CVE-2026-42587	7.5 HIGH
CVE-2026-42779	9.8 CRITICAL
CVE-2026-55956	6.5 MEDIUM
CVE-2026-59084	9.1 CRITICAL
CVE-2026-71142	7.5 HIGH
CVE-2026-71143	7.4 HIGH

CWE's

CWE	Beschrijving
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-1059	Insufficient Technical Documentation
CWE-1104	Use of Unmaintained Third Party Components
CWE-1131	CISQ Quality Measures (2016) - Security
CWE-1395	Dependency on Vulnerable Third-Party Component
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-226	Sensitive Information in Resource Not Removed Before Reuse
CWE-285	Improper Authorization
CWE-287	Improper Authentication

CWE-400	Uncontrolled Resource Consumption
CWE-416	Use After Free
CWE-502	Deserialization of Untrusted Data
CWE-551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-787	Out-of-bounds Write

Getroffen producten

Oracle
Oracle Communications
Oracle Communications BRM - Elastic Charging Engine
Oracle Communications Billing and Revenue Management
Oracle Communications Cloud Native Core Binding Support Function
Oracle Communications Cloud Native Core DBTier
Oracle Communications Cloud Native Core Network Exposure Function
Oracle Communications Cloud Native Core Network Repository Function
Oracle Communications Cloud Native Core Network Slice Selection Function
Oracle Communications Cloud Native Core Policy
Oracle Communications Cloud Native Core Security Edge Protection Proxy

Oracle Communications Cloud Native Core Service Communication Proxy
Oracle Communications Cloud Native Core Unified Data Repository
Oracle Communications Network Analytics Data Director
Oracle Communications Network Charging and Control
Oracle Communications Network Integrity
Oracle Communications Order and Service Management
Oracle Communications Service Catalog and Design
Oracle Communications Unified Assurance
Oracle Communications Unified Inventory Management

Disclaimer