



NCSC-2026-0022

Kwetsbaarheden verholpen in Oracle Communications producten

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 21-01-2026

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 producten.

Duiding

De kwetsbaarheden stellen aanvallers in staat om ongeautoriseerde toegang te krijgen tot het systeem, wat kan leiden tot gegevensmanipulatie en gedeeltelijke denial-of-service. De aanvallers kunnen deze kwetsbaarheden misbruiken via HTTP-verzoeken, wat mogelijk resulteert in een significante impact op de beschikbaarheid en integriteit van de gegevens.

Oplossingen

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

Referenties

➤ <https://www.oracle.com/security-alerts/cpujan2026.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-12133	6.9 MEDIUM
➤ CVE-2024-46901	5.1 MEDIUM
➤ CVE-2025-5115	7.7 HIGH
➤ CVE-2025-5318	5.3 MEDIUM
➤ CVE-2025-5987	5.1 MEDIUM
➤ CVE-2025-8194	7.5 HIGH
➤ CVE-2025-8916	6.3 MEDIUM
➤ CVE-2025-9900	5.3 MEDIUM
➤ CVE-2025-25193	4.8 MEDIUM

> CVE-2025-26333	5.9 MEDIUM
> CVE-2025-27533	6.9 MEDIUM
> CVE-2025-32988	6.3 MEDIUM
> CVE-2025-32990	6.9 MEDIUM
> CVE-2025-41249	7.5 HIGH
> CVE-2025-46727	6.9 MEDIUM
> CVE-2025-48060	7.7 HIGH
> CVE-2025-48734	8.1 HIGH
> CVE-2025-48924	6.5 MEDIUM
> CVE-2025-48976	8.7 HIGH
> CVE-2025-49844	5.3 MEDIUM
> CVE-2025-54571	6.9 MEDIUM
> CVE-2025-55163	8.2 HIGH
> CVE-2025-58057	6.9 MEDIUM
> CVE-2025-58098	6.3 MEDIUM
> CVE-2025-59375	6.9 MEDIUM
> CVE-2025-61795	2.3 LOW
> CVE-2025-64718	5.3 MEDIUM
> CVE-2025-65018	5.3 MEDIUM
> CVE-2025-66418	8.9 HIGH
> CVE-2025-66516	10.0 CRITICAL
> CVE-2025-68161	6.3 MEDIUM

CWE's

CWE	Beschrijving
➤ CWE-863	Incorrect Authorization
➤ CWE-937	CWE-937
➤ CWE-1035	CWE-1035
➤ CWE-1321	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')
➤ CWE-20	Improper Input Validation
➤ CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
➤ CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
➤ CWE-116	Improper Encoding or Escaping of Output
➤ CWE-121	Stack-based Buffer Overflow
➤ CWE-122	Heap-based Buffer Overflow
➤ CWE-123	Write-what-where Condition
➤ CWE-125	Out-of-bounds Read
➤ CWE-126	Buffer Over-read
➤ CWE-201	Insertion of Sensitive Information Into Sent Data
➤ CWE-209	Generation of Error Message Containing Sensitive Information
➤ CWE-252	Unchecked Return Value
➤ CWE-284	Improper Access Control
➤ CWE-285	Improper Authorization
➤ CWE-295	Improper Certificate Validation
➤ CWE-297	Improper Validation of Certificate with Host Mismatch
➤ CWE-393	Return of Wrong Status Code
➤ CWE-400	Uncontrolled Resource Consumption

➤ CWE-404	Improper Resource Shutdown or Release
➤ CWE-407	Inefficient Algorithmic Complexity
➤ CWE-409	Improper Handling of Highly Compressed Data (Data Amplification)
➤ CWE-415	Double Free
➤ CWE-416	Use After Free
➤ CWE-611	Improper Restriction of XML External Entity Reference
➤ CWE-674	Uncontrolled Recursion
➤ CWE-770	Allocation of Resources Without Limits or Throttling
➤ CWE-787	Out-of-bounds Write
➤ CWE-789	Memory Allocation with Excessive Size Value
➤ CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')

Getroffen producten

Oracle
Communications
Oracle Cloud Native Session Border Controller
Oracle Communications ASAP
Oracle Communications BRM - Elastic Charging Engine
Oracle Communications Billing and Revenue Management
Oracle Communications Element Manager
Oracle Communications IP Service Activator

Oracle Communications Network Analytics Data Director
Oracle Communications Network Integrity
Oracle Communications Operations Monitor
Oracle Communications Order and Service Management
Oracle Communications Policy Management
Oracle Communications Pricing Design Center
Oracle Communications Session Border Controller
Oracle Communications Session Report Manager
Oracle Communications Unified Assurance
Oracle Communications Unified Inventory Management
Oracle Enterprise Communications Broker

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.