Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0498

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Oracle Communications

Publicatiedatum: 18-11-2026

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 de-len. 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 kwetsbaarheden verholpen in onder andere Oracle Communications Unified Assurance, Oracle Communications Billing and Revenue Management, Oracle Primavera Unifier, en Oracle Java SE. Daarnaast zijn fixes uitgebracht voor Ruby-componenten in Oracle Communication producten zoals Net::IMAP, Mail, Nokogiri, rubyzip en MessagePack, Node.js, OpenSSL, Curl, Libgcrypt, Libexpat, Puma, Containerd, Faraday, go-git, PCRE2, Apache Tomcat, Apache HTTP Server, Perl DBI, nghttp2, en andere open source libraries en tools.

Duiding

De kwetsbaarheden omvatten diverse typen beveiligingsproblemen zoals incorrecte cryptografische berekeningen, onvoldoende toegangsbeperkingen, heap buffer overflows, use-after-free fouten, denial-of-service door crashes of resource leaks, command injection, path traversal, memory corruptie, integer overflows, en onjuiste validatie van input. Aanvallers kunnen deze kwetsbaarheden misbruiken om onder meer ongeautoriseerde toegang te verkrijgen, gevoelige informatie te lekken, data te wijzigen, systemen te laten crashen, denial-of-service te veroorzaken, of in sommige gevallen volledige systeemcompromittering te bereiken. Sommige kwetsbaarheden vereisen authentificatie, andere kunnen door onbevoegde netwerkaanvallers worden geëxploiteerd. Er zijn ook kwetsbaarheden die specifiek impact hebben op bepaalde configuraties of functies, zoals persistent connections in Puma of OAuth token refresh in RabbitMQ.

Oplossingen

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

Referenties

- https://www.oracle.com/security-alerts/cspunov2026.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-1229	2.9 LOW
CVE-2026-3198	7.1 HIGH
CVE-2026-9076	7.5 HIGH
CVE-2026-9547	9.8 CRITICAL
CVE-2026-22018	3.7 LOW
CVE-2026-27135	7.5 HIGH
CVE-2026-41889	2.3 LOW
CVE-2026-41989	7.5 HIGH
CVE-2026-47242	5.8 MEDIUM
CVE-2026-47737	7.5 HIGH
CVE-2026-53495	6.8 MEDIUM
CVE-2026-54297	7.5 HIGH
CVE-2026-54522	2.1 LOW
CVE-2026-57438	2.2 LOW
CVE-2026-63435	5.3 MEDIUM
CVE-2026-67420	2.3 LOW
CVE-2026-71557	6.3 MEDIUM
CVE-2026-76957	7.8 HIGH
CVE-2026-85396	8.7 HIGH
CVE-2026-87022	7.5 HIGH
CVE-2026-88816	7.5 HIGH
CVE-2026-89161	7.8 HIGH
CVE-2026-91777	7.5 HIGH
CVE-2026-93546	8.8 HIGH
CVE-2026-102278	7.5 HIGH
CVE-2026-111497	9.2 CRITICAL
CVE-2026-114820	9.1 CRITICAL

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory
CWE-77	Improper Neutralization of Special Elements used in a Command
CWE-89	Improper Neutralization of Special Elements used in an SQL Command
CWE-93	Improper Neutralization of CRLF Sequences
CWE-125	Out-of-bounds Read
CWE-130	Improper Handling of Length Parameter Inconsistency
CWE-131	Incorrect Calculation of Buffer Size
CWE-190	Integer Overflow or Wraparound
CWE-252	Unchecked Return Value
CWE-266	Incorrect Privilege Assignment
CWE-290	Authentication Bypass by Spoofing
CWE-295	Improper Certificate Validation
CWE-297	Improper Validation of Certificate with Host Mismatch
CWE-327	Use of a Broken or Risky Cryptographic Algorithm
CWE-347	Improper Verification of Cryptographic Signature
CWE-358	Improperly Implemented Security Check for Standard
CWE-416	Use After Free
CWE-425	Direct Request
CWE-436	Interpretation Conflict
CWE-590	Free of Memory not on the Heap
CWE-606	Unchecked Input for Loop Condition
CWE-617	Reachable Assertion
CWE-674	Uncontrolled Recursion
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-772	Missing Release of Resource after Effective Lifetime
CWE-787	Out-of-bounds Write
CWE-825	Expired Pointer Dereference
CWE-843	Access of Resource Using Incompatible Type
CWE-862	Missing Authorization

CWE	Beschrijving
CWE-1341	Multiple Releases of Same Resource or Handle

Getroffen producten

Oracle
Communications

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.