Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0375

Kwetsbaarheden verholpen in Oracle Communications

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 16-09-2026

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 31 kwetsbaarheden verholpen in diverse Oracle Communications-producten, waaronder Oracle Communications Unified Assurance, Oracle Communications Cloud Native Core Security Edge Protection Proxy, Oracle Communications MetaSolv Solution Module - ASR, 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. Van de in totaal 31 kwetsbaarheden zijn vier als kritiek aangemerkt en kunnen 23 kwetsbaarheden zonder authenticatie op afstand worden misbruikt. Succesvol misbruik kan onder meer leiden tot het verkrijgen van ongeautoriseerde toegang tot gevoelige informatie, het wijzigen van gegevens en het verstoren van de beschikbaarheid van getroffen systemen. Sommige kwetsbaarheden vereisen gebruikersinteractie of voorafgaande toegangsrechten, terwijl andere volledig op afstand en zonder authenticatie kunnen worden misbruikt.

De vier kwetsbaarheden die als kritiek zijn aangemerkt, CVE-2026-44024, CVE-2026-17544, CVE-2026-71290 en CVE-2026-73194, hebben een CVSS-score van 9,1 of hoger en bevinden zich in verschillende Core-componenten van Oracle Communications Unified Assurance, waaronder Fluentd, PHP, Apache HttpClient en DBI. Deze kwetsbaarheden kunnen zonder authenticatie op afstand worden misbruikt en kunnen een hoge impact hebben op de vertrouwelijkheid en, afhankelijk van de kwetsbaarheid, de integriteit en beschikbaarheid van getroffen systemen.

Het NCSC adviseert om de beveiligingsupdates voor de kritieke kwetsbaarheden met voorrang toe te passen.

Oplossingen

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

Referenties

- https://www.oracle.com/security-alerts/cspusep2026.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-9563	7.5 HIGH
CVE-2026-12590	5.9 MEDIUM
CVE-2026-13006	7.0 HIGH
CVE-2026-13758	3.7 LOW
CVE-2026-17544	8.1 HIGH
CVE-2026-19880	6.3 MEDIUM
CVE-2026-34477	6.3 MEDIUM
CVE-2026-39822	7.8 HIGH
CVE-2026-41239	6.8 MEDIUM
CVE-2026-41989	7.5 HIGH
CVE-2026-44024	9.8 CRITICAL
CVE-2026-48998	5.3 MEDIUM
CVE-2026-49284	7.1 HIGH
CVE-2026-49844	6.3 MEDIUM
CVE-2026-50734	7.5 HIGH
CVE-2026-54518	8.1 HIGH
CVE-2026-55952	8.2 HIGH
CVE-2026-57220	7.5 HIGH
CVE-2026-58520	6.9 MEDIUM
CVE-2026-59943	6.3 MEDIUM
CVE-2026-61109	6.5 MEDIUM

CVE-2026-63308	5.3 MEDIUM
CVE-2026-64849	9.3 CRITICAL
CVE-2026-66299	7.5 HIGH
CVE-2026-67355	8.2 HIGH
CVE-2026-71290	9.1 CRITICAL
CVE-2026-73194	9.1 CRITICAL
CVE-2026-73508	7.5 HIGH
CVE-2026-83417	7.1 HIGH
CVE-2026-83418	8.2 HIGH
CVE-2026-83419	5.4 MEDIUM

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-61	UNIX Symbolic Link (Symlink) Following
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-116	Improper Encoding or Escaping of Output
CWE-129	Improper Validation of Array Index
CWE-130	Improper Handling of Length Parameter Inconsistency
CWE-131	Incorrect Calculation of Buffer Size
CWE-201	Insertion of Sensitive Information Into Sent Data

CWE-208	Observable Timing Discrepancy
CWE-209	Generation of Error Message Containing Sensitive Information
CWE-295	Improper Certificate Validation
CWE-297	Improper Validation of Certificate with Host Mismatch
CWE-404	Improper Resource Shutdown or Release
CWE-456	Missing Initialization of a Variable
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
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-789	Memory Allocation with Excessive Size Value
CWE-863	Incorrect Authorization
CWE-918	Server-Side Request Forgery (SSRF)
CWE-941	Incorrectly Specified Destination in a Communication Channel
CWE-1284	Improper Validation of Specified Quantity in Input
CWE-1286	Improper Validation of Syntactic Correctness of Input
CWE-1289	Improper Validation of Unsafe Equivalence in Input

Getroffen producten

Oracle
Oracle Communications
Oracle Communications Cloud Native Core Console
Oracle Communications MetaSolv Solution Module - ASR

Oracle Communications Operations Monitor
Oracle Communications Service Catalog and Design
Oracle Communications Unified Assurance

Disclaimer