Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0330

Kwetsbaarheden verholpen in Oracle Communications producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 23-10-2025

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 meerdere kwetsbaarheden verholpen in zijn Communications producten, waaronder de Unified Assurance en Cloud Native Core.

Duiding

De kwetsbaarheden in de Oracle Communications producten stellen kwaadwillenden in staat om ongeautoriseerde toegang te verkrijgen, wat kan leiden tot gedeeltelijke of volledige Denial-of-Service (DoS) aanvallen. Specifiek kunnen aanvallers met netwerktoegang de systemen compromitteren, wat resulteert in ongeautoriseerde toegang tot gevoelige gegevens. De CVSS-scores van deze kwetsbaarheden variëren van 3.1 tot 9.8, wat wijst op een breed scala aan risico's, van beperkte tot ernstige impact op de vertrouwelijkheid, integriteit en beschikbaarheid van de systemen.

Oplossingen

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

Referenties

- https://www.oracle.com/security-alerts/cpuoct2025.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2023-26555	6.4 MEDIUM
CVE-2024-7254	8.7 HIGH
CVE-2024-8006	4.6 MEDIUM
CVE-2024-12133	6.9 MEDIUM
CVE-2024-28182	7.5 HIGH
CVE-2024-35164	2.3 LOW
CVE-2024-37371	9.1 CRITICAL

CVE-2024-47554	8.7 HIGH
CVE-2024-50609	7.5 HIGH
CVE-2024-51504	8.8 HIGH
CVE-2024-57699	5.1 MEDIUM
CVE-2025-1948	7.5 HIGH
CVE-2025-3576	5.9 MEDIUM
CVE-2025-4373	5.1 MEDIUM
CVE-2025-4517	6.9 MEDIUM
CVE-2025-4802	7.3 HIGH
CVE-2025-5115	7.7 HIGH
CVE-2025-5318	5.3 MEDIUM
CVE-2025-5399	5.3 MEDIUM
CVE-2025-5889	1.3 LOW
CVE-2025-6965	7.2 HIGH
CVE-2025-7339	3.4 LOW
CVE-2025-7425	2.0 LOW
CVE-2025-7962	6.0 MEDIUM
CVE-2025-8058	5.9 MEDIUM
CVE-2025-8916	6.3 MEDIUM
CVE-2025-9086	2.3 LOW
CVE-2025-25724	2.3 LOW
CVE-2025-27210	6.9 MEDIUM
CVE-2025-27533	6.9 MEDIUM

CVE-2025-27553	5.3 MEDIUM
CVE-2025-27587	1.0 LOW
CVE-2025-27817	6.2 MEDIUM
CVE-2025-32415	2.0 LOW
CVE-2025-32728	4.8 MEDIUM
CVE-2025-32990	6.9 MEDIUM
CVE-2025-48734	8.1 HIGH
CVE-2025-48924	6.5 MEDIUM
CVE-2025-48976	8.7 HIGH
CVE-2025-48989	6.9 MEDIUM
CVE-2025-49796	5.3 MEDIUM
CVE-2025-52999	8.7 HIGH
CVE-2025-53547	8.6 HIGH
CVE-2025-53643	6.3 MEDIUM
CVE-2025-53864	6.9 MEDIUM
CVE-2025-54090	6.9 MEDIUM
CVE-2025-55163	8.2 HIGH
CVE-2025-57803	8.8 HIGH
CVE-2025-58057	6.9 MEDIUM
CVE-2025-59375	6.9 MEDIUM

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-23	Relative Path Traversal
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-121	Stack-based Buffer Overflow
CWE-122	Heap-based Buffer Overflow
CWE-124	Buffer Underwrite ('Buffer Underflow')
CWE-125	Out-of-bounds Read
CWE-129	Improper Validation of Array Index
CWE-130	Improper Handling of Length Parameter Inconsistency
CWE-147	Improper Neutralization of Input Terminators
CWE-190	Integer Overflow or Wraparound
CWE-197	Numeric Truncation Error
CWE-241	Improper Handling of Unexpected Data Type
CWE-252	Unchecked Return Value
CWE-253	Incorrect Check of Function Return Value
CWE-284	Improper Access Control
CWE-287	Improper Authentication
CWE-290	Authentication Bypass by Spoofing
CWE-328	Use of Weak Hash
CWE-385	Covert Timing Channel
CWE-390	Detection of Error Condition Without Action

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-426	Untrusted Search Path
CWE-440	Expected Behavior Violation
CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
CWE-476	NULL Pointer Dereference
CWE-674	Uncontrolled Recursion
CWE-697	Incorrect Comparison
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')
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-918	Server-Side Request Forgery (SSRF)
CWE-937	CWE-937
CWE-1035	CWE-1035
CWE-1284	Improper Validation of Specified Quantity in Input
CWE-1333	Inefficient Regular Expression Complexity

Getroffen producten

Oracle
Communications Cloud Native Core Console
Management Cloud Engine
Oracle Communications Billing and Revenue Management
Oracle Communications Calendar Server
Oracle Communications Cloud Native Core Automated Test Suite
Oracle Communications Cloud Native Core Binding Support Function
Oracle Communications Cloud Native Core Certificate Management
Oracle Communications Cloud Native Core DBTier
Oracle Communications Cloud Native Core Network Function Cloud Native Environment
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 Converged Charging System
Oracle Communications Convergence
Oracle Communications Convergent Charging Controller
Oracle Communications Diameter Signaling Router
Oracle Communications EAGLE Element Management System
Oracle Communications EAGLE LNP Application Processor
Oracle Communications LSMS
Oracle Communications Messaging Server
Oracle Communications Network Analytics Data Director
Oracle Communications Network Charging and Control
Oracle Communications Network Integrity
Oracle Communications Offline Mediation Controller
Oracle Communications Operations Monitor
Oracle Communications Order and Service Management
Oracle Communications Pricing Design Center

Oracle Communications Service Catalog and Design
Oracle Communications Session Border Controller
Oracle Communications Unified Assurance
Oracle Communications Unified Inventory Management
Oracle Enterprise Communications Broker
Oracle Enterprise Operations Monitor

Disclaimer