Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0124

Kwetsbaarheden verholpen in Oracle Communications

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 16-04-2025

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 Oracle Communications producten, waaronder de Cloud Native Core en Policy Management.

Duiding

De kwetsbaarheden in Oracle Communications producten stellen ongeauthenticeerde aanvallers in staat om ongeautoriseerde toegang te verkrijgen tot gevoelige gegevens en kunnen leiden tot Denial-of-Service (DoS) aanvallen. Specifieke versies van de Cloud Native Core, zoals de Binding Support Function en Network Repository Function, zijn getroffen, met CVSS-scores die variëren van 4.3 tot 9.8, wat wijst op significante risico's voor de beschikbaarheid en vertrouwelijkheid van de systemen.

Oplossingen

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

Referenties

- https://www.oracle.com/security-alerts/cpuapr2025.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2023-5388	6.5 MEDIUM
CVE-2023-5685	7.5 HIGH
CVE-2023-49582	4.8 MEDIUM
CVE-2023-51074	7.5 HIGH
CVE-2024-1135	8.2 HIGH
CVE-2024-4227	7.5 HIGH
CVE-2024-5535	9.1 CRITICAL
CVE-2024-6763	

CVE-2024-7254	8.7 HIGH
CVE-2024-11053	9.1 CRITICAL
CVE-2024-12797	7.4 HIGH
CVE-2024-12798	5.9 MEDIUM
CVE-2024-21538	8.7 HIGH
CVE-2024-25638	7.0 HIGH
CVE-2024-28168	6.9 MEDIUM
CVE-2024-28219	7.3 HIGH
CVE-2024-28834	5.3 MEDIUM
CVE-2024-31141	6.8 MEDIUM
CVE-2024-34064	5.4 MEDIUM
CVE-2024-35195	5.7 MEDIUM
CVE-2024-37891	4.4 MEDIUM
CVE-2024-38819	6.9 MEDIUM
CVE-2024-38827	6.3 MEDIUM
CVE-2024-40896	9.8 CRITICAL
CVE-2024-43044	7.1 HIGH
CVE-2024-43709	
CVE-2024-43796	6.3 MEDIUM
CVE-2024-47072	7.7 HIGH
CVE-2024-47554	8.7 HIGH
CVE-2024-49767	6.9 MEDIUM
CVE-2024-50602	5.1 MEDIUM

CVE-2024-52046	10.0 CRITICAL
CVE-2024-52303	8.7 HIGH
CVE-2024-53122	5.9 MEDIUM
CVE-2024-56128	1.7 LOW
CVE-2024-56337	7.2 HIGH
CVE-2024-57699	5.1 MEDIUM
CVE-2025-1974	9.8 CRITICAL
CVE-2025-23084	4.8 MEDIUM
CVE-2025-23184	
CVE-2025-24813	9.2 CRITICAL
CVE-2025-24928	7.8 HIGH
CVE-2025-24970	6.9 MEDIUM
CVE-2025-27516	7.3 HIGH
CVE-2025-27789	6.2 MEDIUM
CVE-2025-30729	5.5 MEDIUM
CVE-2025-31721	4.9 MEDIUM

CWE's

CWE	Beschrijving
CWE-44	Path Equivalence: 'file.name' (Internal Dot)
CWE-706	Use of Incorrectly-Resolved Name or Reference
CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
CWE-1321	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')

CWE-502	Deserialization of Untrusted Data
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-121	Stack-based Buffer Overflow
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-1395	Dependency on Vulnerable Third-Party Component
CWE-653	Improper Isolation or Compartmentalization
CWE-670	Always-Incorrect Control Flow Implementation
CWE-676	Use of Potentially Dangerous Function
CWE-1336	Improper Neutralization of Special Elements Used in a Template Engine
CWE-392	Missing Report of Error Condition
CWE-772	Missing Release of Resource after Effective Lifetime
CWE-208	Observable Timing Discrepancy
CWE-669	Incorrect Resource Transfer Between Spheres
CWE-349	Acceptance of Extraneous Untrusted Data With Trusted Data
CWE-834	Excessive Iteration
CWE-303	Incorrect Implementation of Authentication Algorithm
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-917	Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')
CWE-1286	Improper Validation of Syntactic Correctness of Input
CWE-754	Improper Check for Unusual or Exceptional Conditions
CWE-680	Integer Overflow to Buffer Overflow
CWE-345	Insufficient Verification of Data Authenticity
CWE-369	Divide By Zero

CWE-552	Files or Directories Accessible to External Parties
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-404	Improper Resource Shutdown or Release
CWE-862	Missing Authorization
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-1333	Inefficient Regular Expression Complexity
CWE-295	Improper Certificate Validation
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-327	Use of a Broken or Risky Cryptographic Algorithm
CWE-400	Uncontrolled Resource Consumption
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-674	Uncontrolled Recursion
CWE-611	Improper Restriction of XML External Entity Reference
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-269	Improper Privilege Management
CWE-20	Improper Input Validation

Getroffen producten

Oracle
Communications Cloud Native Core Binding Support Function
Communications Cloud Native Core Policy

Communications Cloud Native Core Console
Communications Cloud Native Core Security Edge Protection Proxy
Communications Unified Assurance
Management Cloud Engine
Communications Cloud Native Core Network Data Analytics Function
Communications Cloud Native Core Network Function Cloud Native Environment
Communications Element Manager
Communications Policy Management
Communications Session Report Manager
SD-WAN Edge
Communications Cloud Native Core Unified Data Repository
Communications Session Border Controller
Enterprise Communications Broker
Oracle Communications Cloud Native Core Binding Support Function
Oracle Communications Cloud Native Core DBTier
Oracle Communications Cloud Native Core Policy

Oracle Communications Cloud Native Core Certificate Management
Oracle Communications Cloud Native Core Console
Oracle Communications Cloud Native Core Network Repository Function
Oracle Communications Cloud Native Core Security Edge Protection Proxy
Oracle Communications Cloud Native Core Service Communication Proxy
Oracle Communications EAGLE Element Management System
Oracle Communications Operations Monitor
Oracle Communications User Data Repository
Oracle Communications Diameter Signaling Router
Oracle Communications Cloud Native Core Network Data Analytics Function
Oracle Communications Cloud Native Core Network Function Cloud Native Environment
Oracle Communications Element Manager
Oracle Communications Policy Management
Oracle Communications Session Report Manager
Oracle SD-WAN Edge
Oracle Communications Cloud Native Core Unified Data Repository

Oracle Communications Session Border Controller
Oracle Enterprise Communications Broker
Oracle Communications Network Analytics Data Director
Oracle Communications Network Integrity
Oracle Communications Unified Assurance
Oracle Communications Billing and Revenue Management
Oracle Communications Messaging Server
Oracle Communications MetaSolv Solution
Oracle Communications Network Charging and Control
Oracle Communications Order and Service Management
Oracle Communications Pricing Design Center
Oracle Communications Service Catalog and Design
Oracle Communications Unified Inventory Management
Oracle Corporation
Oracle Communications Order and Service Management

Disclaimer