Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0021

Kwetsbaarheden verholpen in Oracle Communications

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 22-01-2025

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 Communicatieproducten, waaronder Oracle Communications Unified Assurance, Oracle Communications Cloud Native Core Network Function en Oracle Communications Order and Service Management.

Duiding

De kwetsbaarheden stellen ongeauthenticeerde kwaadwillenden in staat om Denial of Service (DoS) aanvallen uit te voeren of om ongeautoriseerde toegang tot gevoelige gegevens te verkrijgen. Specifieke versies, zoals 24.2.0 en 24.3.0 van de Cloud Native Core Network Function, zijn bijzonder kwetsbaar. Kwaadwillenden kunnen deze kwetsbaarheden misbruiken door speciaal geprepareerde HTTP-verzoeken te sturen naar het kwetsbare systeem.

Oplossingen

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

Referenties

- https://www.oracle.com/security-alerts/cpujan2025.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2022-41727	
CVE-2023-4408	
CVE-2023-5678	
CVE-2023-5981	5.9 MEDIUM
CVE-2023-6597	7.8 HIGH
CVE-2023-7256	4.4 MEDIUM
CVE-2023-29407	6.5 MEDIUM

CVE-2023-29408	6.5 MEDIUM
CVE-2023-40577	7.5 HIGH
CVE-2023-46218	6.5 MEDIUM
CVE-2023-46219	9.8 CRITICAL
CVE-2023-46604	10.0 CRITICAL
CVE-2023-50868	
CVE-2024-0232	
CVE-2024-0397	7.5 HIGH
CVE-2024-0450	6.2 MEDIUM
CVE-2024-1442	6.0 MEDIUM
CVE-2024-2961	8.8 HIGH
CVE-2024-3596	9.0 CRITICAL
CVE-2024-4030	7.5 HIGH
CVE-2024-4032	7.5 HIGH
CVE-2024-5535	9.1 CRITICAL
CVE-2024-6119	9.1 CRITICAL
CVE-2024-6162	7.5 HIGH
CVE-2024-6232	7.5 HIGH
CVE-2024-7254	8.2 HIGH
CVE-2024-7592	7.5 HIGH
CVE-2024-7885	7.5 HIGH
CVE-2024-8006	4.4 MEDIUM
CVE-2024-9143	

CVE-2024-22195	6.1 MEDIUM
CVE-2024-24786	7.5 HIGH
CVE-2024-24791	7.5 HIGH
CVE-2024-25638	8.9 HIGH
CVE-2024-25710	8.1 HIGH
CVE-2024-26308	5.9 MEDIUM
CVE-2024-27309	7.4 HIGH
CVE-2024-28219	7.3 HIGH
CVE-2024-28834	5.3 MEDIUM
CVE-2024-28835	5.3 MEDIUM
CVE-2024-28849	6.5 MEDIUM
CVE-2024-29025	7.3 HIGH
CVE-2024-29131	8.1 HIGH
CVE-2024-29133	7.3 HIGH
CVE-2024-33599	8.6 HIGH
CVE-2024-33600	8.6 HIGH
CVE-2024-33601	8.6 HIGH
CVE-2024-33602	8.6 HIGH
CVE-2024-34064	5.4 MEDIUM
CVE-2024-34750	7.5 HIGH
CVE-2024-35195	5.7 MEDIUM
CVE-2024-37370	9.1 CRITICAL
CVE-2024-37371	9.1 CRITICAL

CVE-2024-37891	4.4 MEDIUM
CVE-2024-38475	
CVE-2024-38807	6.3 MEDIUM
CVE-2024-38809	8.0 HIGH
CVE-2024-38816	8.1 HIGH
CVE-2024-38819	7.5 HIGH
CVE-2024-38820	9.8 CRITICAL
CVE-2024-38827	4.8 MEDIUM
CVE-2024-38998	9.8 CRITICAL
CVE-2024-38999	10.0 CRITICAL
CVE-2024-41817	7.8 HIGH
CVE-2024-45490	9.8 CRITICAL
CVE-2024-45491	9.8 CRITICAL
CVE-2024-45492	9.8 CRITICAL
CVE-2024-47535	5.5 MEDIUM
CVE-2024-47554	7.5 HIGH
CVE-2024-47561	9.8 CRITICAL
CVE-2024-47803	5.3 MEDIUM
CVE-2024-47804	5.3 MEDIUM
CVE-2024-49766	6.5 MEDIUM
CVE-2024-49767	7.5 HIGH
CVE-2024-50379	9.8 CRITICAL
CVE-2024-50602	5.9 MEDIUM

CVE-2024-53677	9.0 CRITICAL
CVE-2024-54677	9.8 CRITICAL
CVE-2024-56337	9.8 CRITICAL
CVE-2025-21542	6.3 MEDIUM
CVE-2025-21544	5.4 MEDIUM
CVE-2025-21554	5.3 MEDIUM

CWE's

CWE	Beschrijving
CWE-1395	Dependency on Vulnerable Third-Party Component
CWE-670	Always-Incorrect Control Flow Implementation
CWE-405	Asymmetric Resource Consumption (Amplification)
CWE-35	Path Traversal: '.../...//'
CWE-466	Return of Pointer Value Outside of Expected Range
CWE-338	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)
CWE-676	Use of Potentially Dangerous Function
CWE-606	Unchecked Input for Loop Condition
CWE-450	Multiple Interpretations of UI Input
CWE-131	Incorrect Calculation of Buffer Size
CWE-328	Use of Weak Hash
CWE-130	Improper Handling of Length Parameter Inconsistency
CWE-669	Incorrect Resource Transfer Between Spheres
CWE-1220	Insufficient Granularity of Access Control
CWE-201	Insertion of Sensitive Information Into Sent Data
CWE-349	Acceptance of Extraneous Untrusted Data With Trusted Data

CWE-755	Improper Handling of Exceptional Conditions
CWE-347	Improper Verification of Cryptographic Signature
CWE-834	Excessive Iteration
CWE-178	Improper Handling of Case Sensitivity
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-440	Expected Behavior Violation
CWE-415	Double Free
CWE-311	Missing Encryption of Sensitive Data
CWE-924	Improper Enforcement of Message Integrity During Transmission in a Communication Channel
CWE-754	Improper Check for Unusual or Exceptional Conditions
CWE-703	Improper Check or Handling of Exceptional Conditions
CWE-617	Reachable Assertion
CWE-427	Uncontrolled Search Path Element
CWE-836	Use of Password Hash Instead of Password for Authentication
CWE-680	Integer Overflow to Buffer Overflow
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-23	Relative Path Traversal
CWE-116	Improper Encoding or Escaping of Output
CWE-345	Insufficient Verification of Data Authenticity
CWE-203	Observable Discrepancy
CWE-354	Improper Validation of Integrity Check Value
CWE-325	Missing Cryptographic Step
CWE-190	Integer Overflow or Wraparound
CWE-451	User Interface (UI) Misrepresentation of Critical Information
CWE-61	UNIX Symbolic Link (Symlink) Following

CWE-552	Files or Directories Accessible to External Parties
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-798	Use of Hard-coded Credentials
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-404	Improper Resource Shutdown or Release
CWE-284	Improper Access Control
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-1333	Inefficient Regular Expression Complexity
CWE-1321	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')
CWE-416	Use After Free
CWE-476	NULL Pointer Dereference
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-502	Deserialization of Untrusted Data
CWE-248	Uncaught Exception
CWE-674	Uncontrolled Recursion
CWE-863	Incorrect Authorization
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-611	Improper Restriction of XML External Entity Reference
CWE-787	Out-of-bounds Write
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-122	Heap-based Buffer Overflow

CWE-121	Stack-based Buffer Overflow
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')
CWE-269	Improper Privilege Management
CWE-20	Improper Input Validation
CWE-209	Generation of Error Message Containing Sensitive Information
CWE-276	Incorrect Default Permissions
CWE-294	Authentication Bypass by Capture-replay
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

oracle
communications
communications__10.4.0.4
communications___23.4.2
communications___23.4.3
communications___23.4.4
communications___23.4.5
communications___23.4.6
communications___24.2.0
communications___7.2.1.0.0
communications___8.6.0.6
communications___8.6.0.8
communications___9.0.2
communications___9.0.3

communications___9.1.1.8.0
communications_applications
communications_applications___12.0.6.0.0
communications_applications___5.5.22
communications_applications___6.0.3
communications_applications___6.0.4
communications_applications___6.0.5
communications_asap
communications_billing_and_revenue_management
communications_brm_- _elastic_charging_engine
communications_cloud_native_core_automated_test_suite
communications_cloud_native_core_binding_support_function
communications_cloud_native_core_certificate_management
communications_cloud_native_core_console
communications_cloud_native_core_dbtier
communications_cloud_native_core_network_data_analytics_function
communications_cloud_native_core_network_exposure_function
communications_cloud_native_core_network_function_cloud_native_environment
communications_cloud_native_core_network_repository_function
communications_cloud_native_core_network_slice_selection_function
communications_cloud_native_core_policy
communications_cloud_native_core_security_edge_protection_proxy
communications_cloud_native_core_service_communication_proxy
communications_cloud_native_core_unified_data_repository
communications_converged_application_server

communications_converged_charging_system
communications_convergence
communications_convergent_charging_controller
communications_core_session_manager
communications_diameter_signaling_router
communications_eagle_element_management_system
communications_element_manager
communications_fraud_monitor
communications_instant_messaging_server
communications_ip_service_activator
communications_messaging_server
communications_metasolv_solution
communications_network_analytics_data_director
communications_network_charging_and_control
communications_network_integrity
communications_offline_mediation_controller
communications_operations_monitor
communications_order_and_service_management
communications_performance_intelligence
communications_policy_management
communications_pricing_design_center
communications_service_catalog_and_design
communications_session_border_controller
communications_session_report_manager
communications_unified_assurance
communications_unified_inventory_management

communications_user_data_repository
communications_webrtc_session_controller

Disclaimer