



NCSC-2024-0414

Kwetsbaarheden verholpen in Oracle Communications

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 17-10-2024

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 kwetsbaarheden verholpen in diverse Communications producten en systemen.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Denial-of-Service (DoS)
- Manipuleren van gegevens
- Uitvoer van willekeurige code (Gebruikersrechten)
- Uitvoer van willekeurige code (Administratorrechten)
- Toegang tot gevoelige gegevens

Oplossingen

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

Referenties

➤ <https://www.oracle.com/security-alerts/cpuoct2024.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2021-37137	7.5 HIGH
➤ CVE-2022-2068	9.8 CRITICAL
➤ CVE-2022-2601	8.6 HIGH
➤ CVE-2022-23437	
➤ CVE-2022-36760	9.8 CRITICAL
➤ CVE-2023-2953	7.5 HIGH
➤ CVE-2023-3635	7.5 HIGH

> CVE-2023-4043	7.5 HIGH
> CVE-2023-5685	7.5 HIGH
> CVE-2023-6597	7.8 HIGH
> CVE-2023-6816	9.8 CRITICAL
> CVE-2023-38408	9.8 CRITICAL
> CVE-2023-43642	7.5 HIGH
> CVE-2023-46136	8.0 HIGH
> CVE-2023-48795	5.9 MEDIUM
> CVE-2023-51775	7.5 HIGH
> CVE-2023-52428	7.5 HIGH
> CVE-2024-0450	6.2 MEDIUM
> CVE-2024-2398	8.6 HIGH
> CVE-2024-4577	9.8 CRITICAL
> CVE-2024-4603	7.5 HIGH
> CVE-2024-5585	9.8 CRITICAL
> CVE-2024-5971	7.5 HIGH
> CVE-2024-6162	7.5 HIGH
> CVE-2024-6387	
> CVE-2024-7254	
> CVE-2024-7264	6.5 MEDIUM
> CVE-2024-22020	8.1 HIGH
> CVE-2024-22201	7.5 HIGH
> CVE-2024-22257	8.2 HIGH

> CVE-2024-22262	8.1 HIGH
> CVE-2024-23672	7.5 HIGH
> CVE-2024-23807	8.1 HIGH
> CVE-2024-24549	7.5 HIGH
> CVE-2024-25062	7.5 HIGH
> CVE-2024-25638	8.9 HIGH
> CVE-2024-26308	5.9 MEDIUM
> CVE-2024-28182	7.5 HIGH
> CVE-2024-28849	6.5 MEDIUM
> CVE-2024-29025	7.3 HIGH
> CVE-2024-29133	7.3 HIGH
> CVE-2024-29736	9.1 CRITICAL
> CVE-2024-29857	7.5 HIGH
> CVE-2024-30251	7.5 HIGH
> CVE-2024-31080	
> CVE-2024-31744	7.5 HIGH
> CVE-2024-32760	7.5 HIGH
> CVE-2024-33602	8.6 HIGH
> CVE-2024-34750	7.5 HIGH
> CVE-2024-37371	9.1 CRITICAL
> CVE-2024-37891	4.4 MEDIUM
> CVE-2024-38816	8.1 HIGH
> CVE-2024-39689	7.5 HIGH

> CVE-2024-40898	7.5 HIGH
> CVE-2024-41817	7.8 HIGH
> CVE-2024-43044	9.0 CRITICAL
> CVE-2024-45492	9.8 CRITICAL

CWE's

CWE	Beschrijving
> CWE-122	Heap-based Buffer Overflow
> CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')
> CWE-20	Improper Input Validation
> CWE-466	Return of Pointer Value Outside of Expected Range
> CWE-606	Unchecked Input for Loop Condition
> CWE-390	Detection of Error Condition Without Action
> CWE-405	Asymmetric Resource Consumption (Amplification)
> CWE-222	Truncation of Security-relevant Information
> CWE-364	Signal Handler Race Condition
> CWE-450	Multiple Interpretations of UI Input
> CWE-130	Improper Handling of Length Parameter Inconsistency
> CWE-772	Missing Release of Resource after Effective Lifetime
> CWE-669	Incorrect Resource Transfer Between Spheres
> CWE-126	Buffer Over-read
> CWE-88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')
> CWE-349	Acceptance of Extraneous Untrusted Data With Trusted Data
> CWE-755	Improper Handling of Exceptional Conditions
> CWE-834	Excessive Iteration

➤ CWE-407	Inefficient Algorithmic Complexity
➤ CWE-754	Improper Check for Unusual or Exceptional Conditions
➤ CWE-703	Improper Check or Handling of Exceptional Conditions
➤ CWE-427	Uncontrolled Search Path Element
➤ CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
➤ CWE-195	Signed to Unsigned Conversion Error
➤ CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
➤ CWE-116	Improper Encoding or Escaping of Output
➤ CWE-345	Insufficient Verification of Data Authenticity
➤ CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
➤ CWE-190	Integer Overflow or Wraparound
➤ CWE-61	UNIX Symbolic Link (Symlink) Following
➤ CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
➤ CWE-125	Out-of-bounds Read
➤ 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-416	Use After Free
➤ CWE-401	Missing Release of Memory after Effective Lifetime
➤ CWE-476	NULL Pointer Dereference
➤ CWE-459	Incomplete Cleanup
➤ CWE-94	Improper Control of Generation of Code ('Code Injection')
➤ CWE-400	Uncontrolled Resource Consumption
➤ CWE-770	Allocation of Resources Without Limits or Throttling

> CWE-248	Uncaught Exception
> CWE-674	Uncontrolled Recursion
> CWE-918	Server-Side Request Forgery (SSRF)
> CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
> CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
> CWE-787	Out-of-bounds Write
> CWE-200	Exposure of Sensitive Information to an Unauthorized Actor

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_billing_and_revenue_management__ - _elastic_charging_engine
communications_brm_- _elastic_charging_engine
communications_calendar_server
communications_cloud_native_configuration_console
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_contacts_server
communications_converged_application_server
communications_converged_application_server_-_service_controller
communications_converged_charging_system
communications_convergence
communications_convergent_charging_controller
communications_core_session_manager
communications_data_model
communications_design_studio
communications_diameter_intelligence_hub
communications_diameter_signaling_router
communications_eagle_application_processor
communications_eagle_element_management_system
communications_eagle_ftp_table_base_retrieval
communications_eagle_lnp_application_processor
communications_eagle_software
communications_elastic_charging_engine
communications_element_manager
communications_evolved_communications_application_server
communications_fraud_monitor
communications_instant_messaging_server
communications_interactive_session_recorder
communications_ip_service_activator
communications_lsms

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_performance_intelligence_center
communications_performance_intelligence_center__pic__software
communications_policy_management
communications_pricing_design_center
communications_service_catalog_and_design
communications_services_gatekeeper
communications_session_border_controller
communications_session_report_manager
communications_session_route_manager
communications_session_router
communications_subscriber-aware_load_balancer
communications_unified_assurance
communications_unified_inventory_management
communications_unified_session_manager
communications_user_data_repository
communications_webrtc_session_controller

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.