Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0293

Kwetsbaarheden verholpen in Oracle Communications Applications

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 17-07-2024

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

Er zijn kwetsbaarheden verholpen in Oracle Communications Applications.

Duiding

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

- Denial-of-Service (DoS)
- Toegang tot gevoelige gegevens
- Toegang tot systeemgegevens
- Manipulatie van gegevens
- Omzeilen van beveiligingsmaatregel
- (Remote) code execution (Gebruikersrechten)

Oplossingen

Oracle heeft updates beschikbaar gesteld om de kwetsbaarheden te verhelpen. Zie de referenties voor meer informatie.

Referenties

- https://nvd.nist.gov/vuln/detail/CVE-2020-13956
- https://nvd.nist.gov/vuln/detail/CVE-2022-34381
- https://nvd.nist.gov/vuln/detail/CVE-2023-29081
- https://nvd.nist.gov/vuln/detail/CVE-2023-35116
- https://nvd.nist.gov/vuln/detail/CVE-2023-44487
- https://nvd.nist.gov/vuln/detail/CVE-2023-46218
- https://nvd.nist.gov/vuln/detail/CVE-2023-48795
- https://nvd.nist.gov/vuln/detail/CVE-2023-5981
- https://nvd.nist.gov/vuln/detail/CVE-2024-0232
- https://nvd.nist.gov/vuln/detail/CVE-2024-22257
- https://nvd.nist.gov/vuln/detail/CVE-2024-22262
- https://nvd.nist.gov/vuln/detail/CVE-2024-23807
- https://nvd.nist.gov/vuln/detail/CVE-2024-27316
- https://nvd.nist.gov/vuln/detail/CVE-2024-29025
- https://nvd.nist.gov/vuln/detail/CVE-2024-29133
- https://www.oracle.com/docs/tech/security-alerts/cpujul2024csaf.json
- https://www.oracle.com/security-alerts/cpujul2024.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2020-13956	5.3 MEDIUM
CVE-2021-29489	5.4 MEDIUM
CVE-2021-37533	7.5 HIGH
CVE-2022-34381	9.8 CRITICAL
CVE-2023-5981	5.9 MEDIUM
CVE-2023-29081	
CVE-2023-35116	7.1 HIGH
CVE-2023-44487	
CVE-2023-46218	6.5 MEDIUM
CVE-2023-48795	5.9 MEDIUM
CVE-2024-0232	
CVE-2024-22257	8.2 HIGH
CVE-2024-22262	8.1 HIGH
CVE-2024-23807	8.1 HIGH
CVE-2024-27316	7.5 HIGH
CVE-2024-29025	
CVE-2024-29133	

CWE's

CWE	Beschrijving
CWE-1329	Reliance on Component That is Not Updateable

CWE-20	Improper Input Validation
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-201	Insertion of Sensitive Information Into Sent Data
CWE-203	Observable Discrepancy
CWE-222	Truncation of Security-relevant Information
CWE-284	Improper Access Control
CWE-400	Uncontrolled Resource Consumption
CWE-404	Improper Resource Shutdown or Release
CWE-416	Use After Free
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-787	Out-of-bounds Write

Getroffen producten

oracle
communications_billing_and_revenue_management
communications_brm__-_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_console
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_- _service_controller
communications_converged_application_server
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_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_center__pic__software
communications_performance_intelligence
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