Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0025

Kwetsbaarheden verholpen in Oracle Financial Services

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 Financial Services en componenten.

Duiding

De kwetsbaarheden stellen ongeauthenticeerde aanvallers in staat om toegang te krijgen tot kritieke gegevens en de systeemintegriteit in gevaar te brengen. Specifieke kwetsbaarheden kunnen leiden tot compromittering van vertrouwelijkheid, integriteit en beschikbaarheid, met schadeclassificaties variërend van gemiddeld tot hoog. Sommige kwetsbaarheden kunnen op afstand worden uitgebuit zonder gebruikersinteractie, wat het risico op privilege-escalatie en denial-of-service vergroot.

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-2022-34169	7.5 HIGH
CVE-2023-26031	
CVE-2023-33201	5.3 MEDIUM
CVE-2023-39410	7.5 HIGH
CVE-2023-44483	6.5 MEDIUM
CVE-2023-48795	7.5 HIGH
CVE-2023-51074	7.5 HIGH
CVE-2023-52070	8.4 HIGH

CVE-2024-28219	7.3 HIGH
CVE-2024-34064	5.4 MEDIUM
CVE-2024-34750	7.5 HIGH
CVE-2024-35195	5.7 MEDIUM
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-2024-45490	9.8 CRITICAL
CVE-2024-45491	9.8 CRITICAL
CVE-2024-45492	9.8 CRITICAL
CVE-2025-21550	6.1 MEDIUM

CWE's

CWE	Beschrijving
CWE-681	Incorrect Conversion between Numeric Types
CWE-20	Improper Input Validation
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-131	Incorrect Calculation of Buffer Size
CWE-178	Improper Handling of Case Sensitivity
CWE-284	Improper Access Control
CWE-1321	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')

CWE-611	Improper Restriction of XML External Entity Reference
CWE-670	Always-Incorrect Control Flow Implementation
CWE-192	Integer Coercion Error
CWE-676	Use of Potentially Dangerous Function
CWE-222	Truncation of Security-relevant Information
CWE-755	Improper Handling of Exceptional Conditions
CWE-704	Incorrect Type Conversion or Cast
CWE-680	Integer Overflow to Buffer Overflow
CWE-426	Untrusted Search Path
CWE-354	Improper Validation of Integrity Check Value
CWE-190	Integer Overflow or Wraparound
CWE-532	Insertion of Sensitive Information into Log File
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-757	Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade')
CWE-400	Uncontrolled Resource Consumption
CWE-502	Deserialization of Untrusted Data
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-121	Stack-based Buffer Overflow
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Getroffen producten

oracle
financial_services_analytical_applications_infrastructure

financial_services_analytical_applications_reconciliation_framework
financial_services_asset_liability_management
financial_services_balance_computation_engine
financial_services_balance_sheet_planning
financial_services_basel_regulatory_capital_basic
financial_services_basel_regulatory_capital_internal_ratings_based_approach
financial_services_behavior_detection_platform
financial_services_cash_flow_engine
financial_services_compliance_studio
financial_services_crime_and_compliance_management_studio
financial_services_currency_transaction_reporting
financial_services_data_governance_for_us_regulatory_reporting
financial_services_data_integration_hub
financial_services_deposit_insurance_calculations_for_liquidity_risk_management
financial_services_enterprise_case_management
financial_services_enterprise_financial_performance_analytics
financial_services_funds_transfer_pricing
financial_services_institutional_performance_analytics
financial_services_lending_and_leasing
financial_services_liquidity_risk_measurement_and_management
financial_services_loan_loss_forecasting_and_provisioning
financial_services_model_management_and_governance
financial_services_profitability_management
financial_services_regulatory_reporting
financial_services_regulatory_reporting_with_agilereporter
financial_services_retail_performance_analytics

financial_services_revenue_management_and_billing
financial_services_trade-based_anti_money_laundering
financial_services_trade-based_anti_money_laundering_enterprise_edition
banking_liquidity_management
banking_origination
banking_corporate_lending_process_management

Disclaimer