



# NCSC-2024-0416

## Kwetsbaarheden verholpen in Oracle Financial Services Applications

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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Feiten

Oracle heeft kwetsbaarheden verholpen in Financial Services Applications.

## Duiding

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

- Cross-Site-Scripting (XSS)
- Denial-of-Service (DoS)
- Manipuleren van data
- 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
➤ <a href="#">CVE-2022-31160</a>	6.1 MEDIUM
➤ <a href="#">CVE-2023-34055</a>	6.5 MEDIUM
➤ <a href="#">CVE-2023-37920</a>	9.8 CRITICAL
➤ <a href="#">CVE-2023-50447</a>	8.1 HIGH
➤ <a href="#">CVE-2024-0232</a>	
➤ <a href="#">CVE-2024-2511</a>	7.5 HIGH

> CVE-2024-5535	9.1 CRITICAL
> CVE-2024-21281	5.3 MEDIUM
> CVE-2024-21284	7.1 HIGH
> CVE-2024-21285	7.1 HIGH
> CVE-2024-22262	8.1 HIGH
> CVE-2024-29025	7.3 HIGH
> CVE-2024-32007	9.1 CRITICAL
> CVE-2024-32114	8.5 HIGH
> CVE-2024-43407	6.1 MEDIUM

## CWE's

CWE	Beschrijving
> CVE-1325	Improperly Controlled Sequential Memory Allocation
> CVE-1188	Initialization of a Resource with an Insecure Default
> CVE-95	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')
> CVE-601	URL Redirection to Untrusted Site ('Open Redirect')
> CVE-345	Insufficient Verification of Data Authenticity
> CVE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
> CVE-404	Improper Resource Shutdown or Release
> CVE-306	Missing Authentication for Critical Function
> CVE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
> CVE-416	Use After Free
> CVE-295	Improper Certificate Validation

➤ 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-200	Exposure of Sensitive Information to an Unauthorized Actor
➤ CWE-20	Improper Input Validation
➤ CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

## Getroffen producten

<b>oracle</b>
banking_apis
banking_branch
banking_cash_management
banking_collections_and_recovery
banking_corporate_lending
banking_corporate_lending_process_management
banking_credit_facilities_process_management
banking_deposits_and_lines_of_credit_servicing
banking_digital_experience
banking_electronic_data_exchange_for_corporates
banking_enterprise_default_management
banking_extensibility_workbench
banking_liquidity_management
banking_loans_servicing
banking_origination
banking_party_management

banking_payments
banking_platform
banking_supply_chain_finance
banking_trade_finance
banking_trade_finance_process_management
banking_treasury_management
banking_virtual_account_management
financial_services_analytical_applications_infrastructure
financial_services_analytical_applications_reconciliation_framework
financial_services_applications
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_with_agilereporter
financial_services_regulatory_reporting
financial_services_retail_performance_analytics
financial_services_revenue_management_and_billing

## 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.