Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0297

Kwetsbaarheden verholpen in Oracle Financial Services 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 Financial Services 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
- (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-2022-36944
- https://nvd.nist.gov/vuln/detail/CVE-2023-26031
- https://nvd.nist.gov/vuln/detail/CVE-2023-34055
- https://nvd.nist.gov/vuln/detail/CVE-2023-44483
- https://nvd.nist.gov/vuln/detail/CVE-2023-47248
- https://nvd.nist.gov/vuln/detail/CVE-2023-50447
- https://nvd.nist.gov/vuln/detail/CVE-2023-51074
- https://nvd.nist.gov/vuln/detail/CVE-2023-52425
- https://nvd.nist.gov/vuln/detail/CVE-2023-6129
- https://nvd.nist.gov/vuln/detail/CVE-2024-21188
- https://nvd.nist.gov/vuln/detail/CVE-2024-22201
- 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-2024-24549
- https://nvd.nist.gov/vuln/detail/CVE-2024-24816
- https://nvd.nist.gov/vuln/detail/CVE-2024-25062
- https://nvd.nist.gov/vuln/detail/CVE-2024-2511
- https://nvd.nist.gov/vuln/detail/CVE-2024-26308

- https://nvd.nist.gov/vuln/detail/CVE-2024-29025
- https://nvd.nist.gov/vuln/detail/CVE-2024-29133
- https://nvd.nist.gov/vuln/detail/CVE-2024-32114
- https://www.oracle.com/docs/tech/security-alerts/cpujul2024csaf.json
- https://www.oracle.com/security-alerts/cpujul2024.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2022-36944	9.8 CRITICAL
CVE-2023-6129	6.5 MEDIUM
CVE-2023-26031	7.5 HIGH
CVE-2023-34055	6.5 MEDIUM
CVE-2023-44483	6.5 MEDIUM
CVE-2023-47248	9.8 CRITICAL
CVE-2023-50447	9.0 CRITICAL
CVE-2023-51074	7.5 HIGH
CVE-2023-52425	7.5 HIGH
CVE-2024-2511	7.5 HIGH
CVE-2024-21188	
CVE-2024-22201	7.5 HIGH
CVE-2024-22262	8.1 HIGH
CVE-2024-23807	8.1 HIGH
CVE-2024-24549	7.5 HIGH
CVE-2024-24816	6.1 MEDIUM
CVE-2024-25062	7.5 HIGH

CVE-2024-26308	5.9 MEDIUM
CVE-2024-29025	
CVE-2024-29133	
CVE-2024-32114	8.5 HIGH

CWE's

CWE	Beschrijving
CWE-1188	Initialization of a Resource with an Insecure Default
CWE-121	Stack-based Buffer Overflow
CWE-20	Improper Input Validation
CWE-306	Missing Authentication for Critical Function
CWE-328	Use of Weak Hash
CWE-400	Uncontrolled Resource Consumption
CWE-404	Improper Resource Shutdown or Release
CWE-416	Use After Free
CWE-426	Untrusted Search Path
CWE-502	Deserialization of Untrusted Data
CWE-532	Insertion of Sensitive Information into Log File
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-787	Out-of-bounds Write
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

oracle
financial_services_analytical_applications_infrastructure
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_enterprise_case_management
financial_services_lending_and_leasing
financial_services_model_management_and_governance
financial_services_revenue_management_and_billing
financial_services_trade-based_anti_money_laundering_enterprise_edition

Disclaimer