



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

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.