



NCSC-2025-0127

Kwetsbaarheden verholpen in Oracle Financial Services

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 16-04-2025

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 kwetsbaarheden verholpen in verschillende Financial Services producten

Duiding

De kwetsbaarheden stellen niet-geauthenticeerde kwaadwillenden in staat om via HTTP toegang te krijgen tot kritieke gegevens, wat kan leiden tot ongeautoriseerde gegevenstoegang en andere beveiligingsrisico's. Kwaadwillenden kunnen ook gebruik maken van misconfiguraties en kwetsbaarheden in de software om privilege-escalatie, denial-of-service en remote code execution uit te voeren.

Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://www.oracle.com/security-alerts/cpuapr2025.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2021-28170	7.5 HIGH
➤ CVE-2023-39410	7.5 HIGH
➤ CVE-2023-49582	4.8 MEDIUM
➤ CVE-2024-5206	5.3 MEDIUM
➤ CVE-2024-28168	6.9 MEDIUM
➤ CVE-2024-28219	7.3 HIGH
➤ CVE-2024-35195	5.7 MEDIUM
➤ CVE-2024-37891	4.4 MEDIUM
➤ CVE-2024-38819	6.9 MEDIUM

> CVE-2024-38820	2.3 LOW
> CVE-2024-38827	6.3 MEDIUM
> CVE-2024-47072	7.7 HIGH
> CVE-2024-47554	8.7 HIGH
> CVE-2024-56128	1.7 LOW
> CVE-2024-56337	7.2 HIGH
> CVE-2024-57699	5.1 MEDIUM
> CVE-2025-21573	6.0 MEDIUM
> CVE-2025-23184	
> CVE-2025-24970	6.9 MEDIUM

CWE's

CWE	Beschrijving
> CVE-670	Always-Incorrect Control Flow Implementation
> CVE-676	Use of Potentially Dangerous Function
> CVE-921	Storage of Sensitive Data in a Mechanism without Access Control
> CVE-922	Insecure Storage of Sensitive Information
> CVE-669	Incorrect Resource Transfer Between Spheres
> CVE-178	Improper Handling of Case Sensitivity
> CVE-303	Incorrect Implementation of Authentication Algorithm
> CVE-732	Incorrect Permission Assignment for Critical Resource
> CVE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
> CVE-680	Integer Overflow to Buffer Overflow
> CVE-639	Authorization Bypass Through User-Controlled Key

➤ CWE-404	Improper Resource Shutdown or Release
➤ CWE-284	Improper Access Control
➤ CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
➤ CWE-400	Uncontrolled Resource Consumption
➤ CWE-502	Deserialization of Untrusted Data
➤ CWE-674	Uncontrolled Recursion
➤ CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
➤ CWE-611	Improper Restriction of XML External Entity Reference
➤ CWE-121	Stack-based Buffer Overflow
➤ CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
➤ CWE-20	Improper Input Validation

Getroffen producten

Oracle
Financial Services Model Management and Governance
Financial Services Analytical Applications Infrastructure
Financial Services Behavior Detection Platform
Banking Liquidity Management
Financial Services Compliance Studio
Oracle Financial Services Model Management and Governance
Oracle Banking APIs

Oracle Banking Digital Experience
Oracle Financial Services Analytical Applications Infrastructure
Oracle Financial Services Revenue Management and Billing
Oracle Banking Corporate Lending Process Management
Oracle Banking Origination
Oracle Financial Services Behavior Detection Platform
Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition
Oracle Banking Liquidity Management
Oracle Financial Services Compliance Studio
Oracle Corporation
Oracle 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.