



NCSC-2025-0333

Kwetsbaarheden verholpen in Oracle Financial Services

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 23-10-2025

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 Oracle Financial Services componenten.

Duiding

De kwetsbaarheden stellen ongeauthenticeerde aanvallers in staat om ongeautoriseerde toegang te krijgen tot gevoelige gegevens via HTTP. Dit kan leiden tot ongeoorloofde toegang en wijzigingen van kritieke data, met een CVSS-score van 9.8 die de significante impact op de vertrouwelijkheid benadrukt. Daarnaast zijn er kwetsbaarheden die kunnen leiden tot denial-of-service (DoS) aanvallen, wat de beschikbaarheid van het systeem in gevaar kan brengen.

Oplossingen

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

Referenties

➤ <https://www.oracle.com/security-alerts/cpuoct2025.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2020-11988	8.2 HIGH
➤ CVE-2024-28168	6.9 MEDIUM
➤ CVE-2025-5115	7.7 HIGH
➤ CVE-2025-6965	7.2 HIGH
➤ CVE-2025-27553	5.3 MEDIUM
➤ CVE-2025-27817	6.2 MEDIUM
➤ CVE-2025-31672	6.9 MEDIUM
➤ CVE-2025-32415	2.0 LOW

> CVE-2025-41249	7.5 HIGH
> CVE-2025-48924	6.5 MEDIUM
> CVE-2025-48976	8.7 HIGH
> CVE-2025-48989	6.9 MEDIUM
> CVE-2025-50074	4.9 MEDIUM
> CVE-2025-50075	6.5 MEDIUM
> CVE-2025-53034	5.4 MEDIUM
> CVE-2025-53035	6.5 MEDIUM
> CVE-2025-53036	8.6 HIGH
> CVE-2025-53037	9.8 CRITICAL
> CVE-2025-55163	8.2 HIGH
> CVE-2025-59375	6.9 MEDIUM
> CVE-2025-61751	8.1 HIGH
> CVE-2025-61756	7.5 HIGH

CWE's

CWE	Beschrijving
> CWE-20	Improper Input Validation
> CWE-23	Relative Path Traversal
> CWE-125	Out-of-bounds Read
> CWE-197	Numeric Truncation Error
> CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CWE-284	Improper Access Control
> CWE-285	Improper Authorization

➤ CWE-306	Missing Authentication for Critical Function
➤ CWE-400	Uncontrolled Resource Consumption
➤ CWE-404	Improper Resource Shutdown or Release
➤ CWE-611	Improper Restriction of XML External Entity Reference
➤ CWE-674	Uncontrolled Recursion
➤ CWE-770	Allocation of Resources Without Limits or Throttling
➤ CWE-862	Missing Authorization
➤ CWE-863	Incorrect Authorization
➤ CWE-918	Server-Side Request Forgery (SSRF)
➤ CWE-937	CWE-937
➤ CWE-1035	CWE-1035
➤ CWE-1284	Improper Validation of Specified Quantity in Input

Getroffen producten

Oracle
Financial Services Revenue Management And Billing
Oracle Banking Branch
Oracle Banking Corporate Lending Process Management
Oracle Banking Origination
Oracle Financial Services Analytical Applications Infrastructure
Oracle Financial Services Behavior Detection Platform
Oracle Financial Services Compliance Studio
Oracle Financial Services Model Management and Governance
Oracle 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.