



NCSC-2026-0025

Kwetsbaarheden verholpen in Oracle Financial Services

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 21-01-2026

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 producten, waaronder Oracle Banking Liquidity Management, Oracle Financial Services Model Management en Oracle FLEXCUBE.

Duiding

De kwetsbaarheden in de Oracle producten stellen ongeauthenticeerde aanvallers in staat om toegang te krijgen tot gevoelige gegevens en Denial-of-Service (DoS) aan te richten. Dit kan leiden tot vertrouwelijkheids- en integriteitsrisico's. Specifieke kwetsbaarheden omvatten onjuist beheer van verbindingen en onvoldoende invoervalidatie wat kan resulteren in systeemcompromittering en serviceonderbrekingen.

Oplossingen

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

Referenties

➤ <https://www.oracle.com/security-alerts/cpujan2026.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-5115	7.7 HIGH
➤ CVE-2025-9230	6.9 MEDIUM
➤ CVE-2025-22228	6.3 MEDIUM
➤ CVE-2025-27817	7.0 HIGH
➤ CVE-2025-41248	7.5 HIGH
➤ CVE-2025-41249	7.5 HIGH
➤ CVE-2025-48734	8.1 HIGH
➤ CVE-2025-48795	5.6 MEDIUM

> CVE-2025-48924	6.5 MEDIUM
> CVE-2025-48976	8.7 HIGH
> CVE-2025-49796	5.3 MEDIUM
> CVE-2025-55163	8.2 HIGH
> CVE-2025-61795	2.3 LOW
> CVE-2025-66418	8.9 HIGH
> CVE-2026-21973	8.1 HIGH
> CVE-2026-21978	6.5 MEDIUM

CWE's

CWE	Beschrijving
> CVE-125	Out-of-bounds Read
> CVE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CVE-284	Improper Access Control
> CVE-285	Improper Authorization
> CVE-287	Improper Authentication
> CVE-289	Authentication Bypass by Alternate Name
> CVE-400	Uncontrolled Resource Consumption
> CVE-404	Improper Resource Shutdown or Release
> CVE-521	Weak Password Requirements
> CVE-674	Uncontrolled Recursion
> CVE-770	Allocation of Resources Without Limits or Throttling
> CVE-787	Out-of-bounds Write
> CVE-843	Access of Resource Using Incompatible Type ('Type Confusion')
> CVE-863	Incorrect Authorization

➤ CWE-918	Server-Side Request Forgery (SSRF)
➤ CWE-937	CWE-937
➤ CWE-1035	CWE-1035

Getroffen producten

Oracle
Oracle Banking Branch
Oracle Banking Cash Management
Oracle Banking Corporate Lending Process Management
Oracle Banking Liquidity Management
Oracle Banking Supply Chain Finance
Oracle FLEXCUBE Investor Servicing
Oracle FLEXCUBE Universal Banking
Oracle Financial Services Compliance Studio
Oracle Financial Services Model Management and Governance
Oracle Insurance Policy Administration J2EE

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.