Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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