Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0258

Kwetsbaarheden verholpen in Oracle Financial Services

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 22-07-2026

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 diverse Financial Services modules. Ook heeft Oracle updates voor diverse third-party-producten verwerkt.

Duiding

De kwetsbaarheden betreffen onder andere code-injectie via malafide schema's in Apache Avro, onbevoegde toegang tot gevoelige data in diverse Oracle producten, en autorisatie-omzeilingen in Spring Security. Verder zijn er problemen met onjuiste verwerking van HTTP-headers in Spring Security, onjuiste validatie van JWT-tokens in Apache Kafka, en onveilige sessiestatusbeheer in Eclipse Jetty. Ook zijn er kwetsbaarheden die leiden tot denial-of-service via resource-uitputting in Apache Netty en urllib3. Sommige kwetsbaarheden kunnen leiden tot volledige systeemcompromittering, ongeautoriseerde datamodificatie, of het lekken van gevoelige informatie. Exploitatie kan plaatsvinden via netwerktoegang, HTTP-verzoeken, of het verwerken van speciaal vervaardigde bestanden of berichten. Voor bepaalde kwetsbaarheden is gebruikersinteractie vereist, terwijl andere op afstand en zonder authenticatie kunnen worden misbruikt.

Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Het wordt aanbevolen om de betreffende producten te updaten naar de gepatchte versies zoals vermeld in de advisories. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.oracle.com/security-alerts/cpujul2026.html
- https://www.oracle.com/security-alerts/cpujul2026verbose.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-47561	9.3 CRITICAL
CVE-2025-33042	6.9 MEDIUM
CVE-2025-41248	7.5 HIGH
CVE-2025-41249	7.5 HIGH

CVE-2025-70873	7.5 HIGH
CVE-2026-4800	9.8 CRITICAL
CVE-2026-5795	2.3 LOW
CVE-2026-21441	8.9 HIGH
CVE-2026-22732	9.1 CRITICAL
CVE-2026-22747	6.8 MEDIUM
CVE-2026-24308	8.7 HIGH
CVE-2026-33557	6.3 MEDIUM
CVE-2026-34481	6.3 MEDIUM
CVE-2026-40976	6.9 MEDIUM
CVE-2026-41044	8.8 HIGH
CVE-2026-44248	7.5 HIGH
CVE-2026-61097	9.6 CRITICAL
CVE-2026-61102	8.1 HIGH
CVE-2026-61105	8.1 HIGH
CVE-2026-61220	6.1 MEDIUM

CWE's

CWE	Beschrijving
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor

Getroffen producten

Oracle
Oracle Banking Branch
Oracle Banking Cash Management
Oracle Banking Corporate Lending
Oracle Banking Corporate Lending Process Management
Oracle Banking Origination
Oracle Banking Trade Finance
Oracle Banking Virtual Account Management
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
Oracle Corporation
Oracle Banking Origination
Oracle Banking Trade Finance

Oracle Banking Trade Finance
Process Management

Disclaimer