Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0312

Kwetsbaarheden verholpen in Oracle Financial Services

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 19-08-2026

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 Enterprise modules.

Duiding

De kwetsbaarheden bevinden zich in Third Party producten, zoals Apache Kafka, Log4j en het Spring Framework, waarvoor eerder door de ontwikkelaars updates zijn uitgebracht. Deze updates zijn nu verwerkt door Oracle in de Financial Services modules die gebruik maken van deze Third Party producten.

Een kwaadwillende kan de kwetsbaarheden misbruiken om toegang te krijgen tot gevoelige gegevens, een Denial-of-Service veroorzaken of om willekeurige code uit te voeren op het kwetsbare systeem.

Oplossingen

Oracle heeft updates uitgebracht voor Financial Services Enterprise Case Management om de genoemde kwetsbaarheden te adresseren. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.oracle.com/security-alerts/cspuaug2026.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-33557	9.1 CRITICAL
CVE-2026-33929	6.6 MEDIUM
CVE-2026-34481	6.3 MEDIUM
CVE-2026-41855	8.1 HIGH
CVE-2026-70922	8.8 HIGH

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-116	Improper Encoding or Escaping of Output
CWE-241	Improper Handling of Unexpected Data Type
CWE-287	Improper Authentication
CWE-303	Incorrect Implementation of Authentication Algorithm
CWE-502	Deserialization of Untrusted Data
CWE-937	OWASP Top Ten 2013 Category A9 - Using Components with Known Vulnerabilities
CWE-1035	OWASP Top Ten 2017 Category A9 - Using Components with Known Vulnerabilities
CWE-1285	Improper Validation of Specified Index, Position, or Offset in Input

Getroffen producten

Oracle
Financial Services Applications
Oracle Financial Services Analytical Applications Infrastructure
Oracle Financial Services Compliance Studio
Oracle Financial Services Model Management and Governance
Oracle Corporation
Oracle Financial Services Enterprise Case Management

Disclaimer