Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0252

Kwetsbaarheden verholpen in Oracle Fusion middleware

NCSC Security Advisory

PRIORITEIT: HOOG

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 een groot aantal kwetsbaarheden verholpen in verschillende Oracle middleware producten, waaronder Oracle Data Integrator, Oracle Coherence, Oracle Access Manager, Oracle Unified Directory, Oracle WebLogic Server Proxy Plug-in, Oracle Fusion Middleware Service Delivery Platform (Messaging Enabler) en Oracle WebCenter Content.

Het totaal aantal kwetsbaarheden dat is verholpen in deze updates is 345.

Duiding

De ernstigste kwetsbaarheden, 9 stuks, hebben de hoogste score van 10.0 gekregen en bevinden zich in diverse Oracle middleware componenten en stellen ongeauthenticeerde externe aanvallers in staat om volledige systeemcompromittering te bereiken.

Aanvallers kunnen via HTTP, LDAP, SOAP of andere netwerkinterfaces willekeurige code uitvoeren of volledige controle over het systeem verkrijgen zonder authenticatie. Sommige kwetsbaarheden kunnen leiden tot ongeautoriseerde toegang, wijziging of verwijdering van kritieke data. De impact kan zich ook uitbreiden naar andere Oracle producten die afhankelijk zijn van de getroffen middleware componenten.

Naast deze 9 kwetsbaarheden met de hoogste score, zijn ook nog eens 145 kwetsbaarheden verholpen met een CVSS score van 9 tot 9.9. Ook van deze kwetsbaarheden is een groot aantal zonder voorafgaande authenticatie op afstand te misbruiken en kunnen leiden tot uitvoer van willekeurige code, toegang tot gevoelige gegevens of volledige systeemcompromittatie.

De overige kwetsbaarheden hebben lagere scores gekregen dan 9. Het voert te ver om alle detailinformatie op de nemen in deze advisory en het NCSC verwijst daarom naar de bijgevoegde referentie.

Door het grote aantal en de ernst van deze kwetsbaarheden acht het NCSC het zeer waarschijnlijk dat grootschalig misbruik op korte termijn plaats gaat vinden. Het NCSC adviseert daarom de bijgevoegde referentie goed door te nemen en de beschikbaar gestelde updates met spoed in te zetten.

Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden in de genoemde middleware producten te verhelpen. 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-2026-47056	10.0 CRITICAL
CVE-2026-60217	10.0 CRITICAL
CVE-2026-60358	10.0 CRITICAL
CVE-2026-60360	10.0 CRITICAL
CVE-2026-60365	10.0 CRITICAL
CVE-2026-60366	
CVE-2026-60379	10.0 CRITICAL
CVE-2026-60389	10.0 CRITICAL
CVE-2026-60644	10.0 CRITICAL

CWE's

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

Getroffen producten

Oracle
Fusion Middleware
Oracle HTTP Server
Oracle Corporation
Oracle Access Manager

Oracle Coherence
Oracle Data Integrator
Oracle Unified Directory
Oracle WebCenter Content
Oracle Weblogic Server Proxy Plug-in
Service Delivery Platform

Disclaimer