Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0377

Kwetsbaarheden verholpen in Oracle Enterprise Manager

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 16-09-2026

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 7 kwetsbaarheden verholpen in diverse Oracle Enterprise Manager-producten, waaronder Oracle Enterprise Manager Base Platform, Oracle Enterprise Manager for Fusion Middleware en Oracle Enterprise Manager for Oracle Database. De beveiligingsupdates zijn niet van toepassing op client-only installaties waarop Oracle Enterprise Manager niet is geïnstalleerd.

Duiding

De kwetsbaarheden betreffen verschillende beveiligingsproblemen in Oracle Enterprise Manager-producten, waaronder mogelijkheden voor niet-geauthenticeerde en laaggeprivilegieerde kwaadwillenden om via netwerktoegang ongeautoriseerde acties uit te voeren. De kwetsbaarheden hebben CVSS-scores variërend van middel tot kritiek. Van de in totaal 7 kwetsbaarheden zijn drie als kritiek aangemerkt en volgens Oracle kunnen vijf kwetsbaarheden zonder authenticatie op afstand worden misbruikt. Succesvol misbruik kan onder meer leiden tot het verkrijgen van ongeautoriseerde toegang tot gevoelige informatie, het wijzigen van gegevens en het verstoren van de beschikbaarheid van getroffen systemen. Sommige kwetsbaarheden vereisen voorafgaande toegangsrechten, terwijl andere volledig op afstand en zonder authenticatie kunnen worden misbruikt.

De drie kwetsbaarheden die als kritiek zijn aangemerkt, CVE-2026-41635, CVE-2026-83355 en CVE-2026-2332, hebben een CVSS-score van 9,1 of hoger en bevinden zich in Agent Next Gen van Oracle Enterprise Manager Base Platform, Metrics van Oracle Enterprise Manager for Fusion Middleware en de Oracle Management Service (OMS) van Oracle Enterprise Manager Base Platform. Deze kwetsbaarheden kunnen volgens Oracle zonder authenticatie op afstand worden misbruikt, vereisen een lage aanvalscomplexiteit en geen gebruikersinteractie. Succesvolle exploitatie kan een hoge impact hebben op de vertrouwelijkheid en integriteit en,ook op de beschikbaarheid van getroffen systemen.

Het NCSC adviseert om de beveiligingsupdates voor de kritieke kwetsbaarheden met voorrang toe te passen.

Oplossingen

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

Referenties

- https://www.oracle.com/security-alerts/cspusep2026.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-68161	6.3 MEDIUM
CVE-2026-2332	9.1 CRITICAL
CVE-2026-41635	9.8 CRITICAL
CVE-2026-49844	6.3 MEDIUM
CVE-2026-62597	6.5 MEDIUM
CVE-2026-83068	7.7 HIGH
CVE-2026-83355	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-116	Improper Encoding or Escaping of Output
CWE-295	Improper Certificate Validation
CWE-297	Improper Validation of Certificate with Host Mismatch
CWE-306	Missing Authentication for Critical Function
CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
CWE-502	Deserialization of Untrusted Data

Getroffen producten

Oracle
Oracle Enterprise Manager Base Platform

Oracle Corporation

Oracle Enterprise Manager for
Fusion Middleware

Disclaimer