Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0311

Kwetsbaarheden verholpen in Oracle Enterprise Manager

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 meerdere kwetsbaarheden verholpen in diverse Oracle Enterprise Manager componenten.

Duiding

De kwetsbaarheden in Oracle Enterprise Manager Base Platform en Oracle Enterprise Manager voor Systems Infrastructure betreffen meerdere problemen waarbij een aanvaller met lage privileges en soms zonder authenticatie via het netwerk of met logon toegang volledige controle kan verkrijgen over het systeem, data kan creëren, verwijderen of wijzigen, en toegang kan krijgen tot gevoelige informatie. Sommige kwetsbaarheden maken privilege escalatie mogelijk. De getroffen versies zijn 13.5 en 24.1 voor Enterprise Manager producten.

Oplossingen

Oracle heeft updates uitgebracht voor Oracle Enterprise Manager Base Platform en Oracle Enterprise Manager voor Systems Infrastructure om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

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

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-2332	9.1 CRITICAL
CVE-2026-34481	6.3 MEDIUM
CVE-2026-60822	7.8 HIGH
CVE-2026-61284	8.8 HIGH
CVE-2026-61286	8.6 HIGH
CVE-2026-61298	5.6 MEDIUM
CVE-2026-61300	7.8 HIGH
CVE-2026-70684	8.1 HIGH

CVE-2026-70737	8.8 HIGH

CWE's

CWE	Beschrijving
CWE-116	Improper Encoding or Escaping of Output
CWE-241	Improper Handling of Unexpected Data Type
CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
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

Getroffen producten

Oracle
Enterprise Manager
Oracle Enterprise Manager Base Platform
Oracle Corporation
Oracle Enterprise Manager for Systems Infrastructure

Disclaimer