Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0257

Kwetsbaarheden verholpen in Oracle Enterprise Manager

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 meerdere kwetsbaarheden verholpen in Oracle Enterprise Manager Base Platform versies 13.5 en 24.1.

Duiding

De kwetsbaarheden in Oracle Enterprise Manager Base Platform stellen aanvallers in staat om via netwerktoegang over HTTPS of HTTP zonder authenticatie of met lage privileges ongeautoriseerde lees-, schrijf-, creatie-, verwijdering- en wijzigingsacties op gevoelige data uit te voeren. Sommige kwetsbaarheden maken het mogelijk om volledige systeemcompromittering te bereiken, waaronder het uitvoeren van willekeurige code en het overnemen van het systeem. Andere kwetsbaarheden kunnen leiden tot gedeeltelijke denial-of-service condities. De kwetsbaarheden zijn aanwezig in verschillende componenten van het platform, zoals Agent Next Gen, Metadata Plugin en UI Framework. Exploitatie kan vereisen dat de aanvaller netwerktoegang heeft en in enkele gevallen gebruikersinteractie. De kwetsbaarheden maken gebruik van onvoldoende toegangscontrole en onjuiste beveiligingsmaatregelen binnen het platform.

Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden in Oracle Enterprise Manager Base Platform 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-2014-3643	8.1 HIGH
CVE-2020-9547	9.8 CRITICAL
CVE-2025-8916	6.3 MEDIUM
CVE-2025-68161	6.3 MEDIUM
CVE-2026-46984	5.3 MEDIUM

CVE-2026-46985	5.3 MEDIUM
CVE-2026-46986	5.3 MEDIUM
CVE-2026-46987	7.7 HIGH
CVE-2026-46988	7.2 HIGH
CVE-2026-46989	9.1 CRITICAL
CVE-2026-46990	10.0 CRITICAL
CVE-2026-46991	4.4 MEDIUM
CVE-2026-46992	8.8 HIGH
CVE-2026-46993	8.2 HIGH
CVE-2026-46994	9.8 CRITICAL
CVE-2026-46995	8.8 HIGH
CVE-2026-46996	7.1 HIGH
CVE-2026-46997	6.5 MEDIUM
CVE-2026-46998	8.8 HIGH
CVE-2026-46999	7.0 HIGH
CVE-2026-47000	3.5 LOW
CVE-2026-47001	5.4 MEDIUM
CVE-2026-47002	6.1 MEDIUM
CVE-2026-47003	5.9 MEDIUM
CVE-2026-47004	8.8 HIGH
CVE-2026-47005	7.2 HIGH
CVE-2026-47006	7.2 HIGH

CWE's

CWE	Beschrijving
CWE-269	Improper Privilege Management
CWE-295	Improper Certificate Validation
CWE-297	Improper Validation of Certificate with Host Mismatch
CWE-502	Deserialization of Untrusted Data
CWE-611	Improper Restriction of XML External Entity Reference
CWE-770	Allocation of Resources Without Limits or Throttling
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
Enterprise Manager Base Platform
Enterprise Manager for Fusion Middleware

Disclaimer