



NCSC-2026-0202

Kwetsbaarheden verholpen in Oracle Enterprise Manager

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 17-06-2026

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 versies 13.5 en 24.1.

Duiding

De kwetsbaarheden in Oracle Enterprise Manager Base Platform versies 13.5 en 24.1 maken het mogelijk voor een aanvaller met lage of geen privileges en netwerktoegang via HTTP of HTTPS om volledige controle over het platform te verkrijgen. Sommige kwetsbaarheden vereisen geen authenticatie en kunnen leiden tot onbevoegde datamodificatie, denial-of-service, of volledige systeemcompromittering. Daarnaast kan een aanvaller met SSH-toegang ook volledige systeemcompromittering bereiken. De kwetsbaarheden kunnen ook impact hebben op andere Oracle-producten die geïntegreerd zijn met het platform. Verder is er een kwetsbaarheid in Apache Log4j's JsonTemplateLayout tot versie 2.25.3 die onjuiste JSON-output genereert bij het serialiseren van niet-eindige floating-point waarden, wat kan leiden tot verstoring van downstream logverwerkende systemen wanneer MapMessages worden gelogd.

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/cspujun2026.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-34481	6.3 MEDIUM
➤ CVE-2026-46832	9.9 CRITICAL
➤ CVE-2026-46852	9.9 CRITICAL
➤ CVE-2026-46853	9.6 CRITICAL
➤ CVE-2026-46854	9.9 CRITICAL
➤ CVE-2026-46855	9.9 CRITICAL

> CVE-2026-46856	9.6 CRITICAL
> CVE-2026-46857	9.8 CRITICAL
> CVE-2026-46858	9.1 CRITICAL
> CVE-2026-46864	8.8 HIGH
> CVE-2026-46865	8.4 HIGH
> CVE-2026-46866	6.9 MEDIUM
> CVE-2026-46867	7.2 HIGH
> CVE-2026-46868	7.2 HIGH
> CVE-2026-46872	5.1 MEDIUM
> CVE-2026-46875	9.1 CRITICAL

CWE's

CWE	Beschrijving
> CVE-116	Improper Encoding or Escaping of Output
> CVE-241	Improper Handling of Unexpected Data Type

Getroffen producten

Oracle
APM - Application Performance Management
Oracle Enterprise Manager Base Platform

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.