



Advisory NCSC-2026-0440

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Oracle Enterprise Manager

Publicatiedatum: 21-10-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Oracle heeft meerdere kwetsbaarheden verholpen in Oracle Enterprise Manager, waaronder de Base Platform, Data Guard Management, Siebel en Virtualization-componenten. De kwetsbaarheden betreffen versies 13.5 en 24.1.

Duiding

De kwetsbaarheden in Oracle Enterprise Manager kunnen leiden tot ongeautoriseerde toegang tot gevoelige gegevens, wijzigingen in data en aantasting van de beschikbaarheid en integriteit van systemen. Sommige kwetsbaarheden maken het mogelijk om willekeurige code uit te voeren. De kwetsbaarheden bevinden zich in verschillende componenten, waaronder Data Guard Management, Base Platform, Siebel en Virtualization. Twee kwetsbaarheden zijn op afstand te misbruiken zonder authenticatie. Voor andere kwetsbaarheden zijn lage gebruikersrechten of lokale toegang vereist.

Oplossingen

Oracle heeft updates uitgebracht voor Oracle Enterprise Manager en gerelateerde componenten om deze kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://www.oracle.com/security-alerts/cpuoct2026.html>

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-48734	9.3 CRITICAL
CVE-2026-54512	8.1 HIGH
CVE-2026-101518	8.8 HIGH
CVE-2026-101525	8.8 HIGH
CVE-2026-101526	8.8 HIGH

CVE	CVSS Score
CVE-2026-101527	7.8 HIGH
CVE-2026-101528	9.9 CRITICAL
CVE-2026-101529	9.9 CRITICAL

CWE's

CWE	Beschrijving
CWE-502	Deserialization of Untrusted Data
CWE-184	Incomplete List of Disallowed Inputs

Getroffen producten

Oracle
Enterprise Manager
Oracle Enterprise Manager Base Platform
Oracle Enterprise Manager for Oracle Database
Oracle Enterprise Manager for Siebel
Oracle Enterprise Manager for Virtualization

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 or 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.