Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0499

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Oracle Enterprise Manager

Publicatiedatum: 18-11-2026

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 de-len. 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 kwetsbaarheden verholpen in Oracle Enterprise Manager Base Platform.

Duiding

In Oracle Enterprise Manager Base Platform (versies 13.5 en 24.1) kan een aanvaller met lage privileges en netwerktoegang via HTTP volledige systeemcompromittering bereiken. In Oracle Enterprise Manager Base Platform Agent Next Gen (versies 13.5 en 24.1) kan een aanvaller met lage infrastructuur login privileges ongeautoriseerde toegang krijgen tot of kritieke data wijzigen. De kwetsbaarheden zijn specifiek voor genoemde versies en componenten. Sommige kwetsbaarheden zijn te misbruiken via netwerktoegang, andere vereisen lage privileges binnen het systeem.

Oplossingen

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

Referenties

- https://www.oracle.com/security-alerts/cspunov2026.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-10050	8.7 HIGH
CVE-2026-114829	8.8 HIGH
CVE-2026-34478	6.9 MEDIUM
CVE-2025-14813	9.3 CRITICAL
CVE-2026-114830	6.1 MEDIUM

CWE's

CWE	Beschrijving
CWE-93	Improper Neutralization of CRLF Sequences
CWE-117	Improper Output Neutralization for Logs
CWE-173	Improper Handling of Alternate Encoding
CWE-303	Incorrect Implementation of Authentication Algorithm
CWE-323	Reusing a Nonce, Key Pair in Encryption
CWE-327	Use of a Broken or Risky Cryptographic Algorithm
CWE-684	Incorrect Provision of Specified Functionality

Getroffen producten

Oracle
Enterprise Manager

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.