



NCSC-2025-0126

Kwetsbaarheden verholpen in Oracle Enterprise Manager

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 16-04-2025

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 kwetsbaarheden verholpen in Oracle Enterprise Manager

Duiding

De kwetsbaarheden stellen ongeauthenticeerde aanvallers in staat om systemen te compromitteren via HTTP of SSH, wat kan leiden tot Denial-of-Service (DoS) of vertrouwelijke informatie openbaarmaking. Specifiek in de ObjectSerializationDecoder van Apache MINA is er een kritieke kwetsbaarheid die op afstand code-executie mogelijk maakt door een gebrek aan beveiligingscontroles in het deserialisatieproces. Dit betreft versies 2.0.X, 2.1.X, en 2.2.X. Daarnaast kunnen aanvallers ook gebruik maken van een kwetsbaarheid in Oracle's Primavera Gateway, die een Denial-of-Service kan veroorzaken.

Oplossingen

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

Referenties

➤ <https://www.oracle.com/security-alerts/cpuapr2025.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2022-45047	9.8 CRITICAL
➤ CVE-2023-1370	7.5 HIGH
➤ CVE-2024-52046	10.0 CRITICAL
➤ CVE-2024-57699	5.1 MEDIUM

CWE's

CWE	Beschrijving
➤ CWE-1124	Excessively Deep Nesting

➤ CWE-404	Improper Resource Shutdown or Release
➤ CWE-94	Improper Control of Generation of Code ('Code Injection')
➤ CWE-502	Deserialization of Untrusted Data
➤ CWE-674	Uncontrolled Recursion

Getroffen producten

Oracle
Enterprise Manager Base Platform
Application Testing Suite
Oracle Enterprise Manager Base Platform
Oracle Application Testing Suite

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.