Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0497

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Oracle Commerce Platform

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 Commerce Platform. Een groot deel hiervan betreft kwetsbaarheden in dependencies, namelijk Apache Neethi, Apache HttpClient en Apache CXF.

Duiding

Oracle Commerce Platform bevat een DoS-kwetsbaarheid die ongeauthenticeerde aanvallers in staat stelt het systeem via HTTP te laten crashen. Verder zijn er in Oracle Primavera Unifier en Oracle SOA Suite vergelijkbare kwetsbaarheden die leiden tot applicatiehangs, crashes of ongeautoriseerde toegang tot data. Tenslotte is er een DoS-kwetsbaarheid in een niet nader genoemd product die wordt gemitigeerd door het beperken van de maximale datahoeveelheid die via API kan worden gelezen.

Oplossingen

Oracle heeft updates uitgebracht voor Oracle Commerce Platform om de genoemde problemen aan te pakken. Zie bijgevoegde referenties voor meer informatie.

Referenties

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

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-42402	7.5 HIGH
CVE-2026-64607	7.5 HIGH
CVE-2026-66144	7.5 HIGH
CVE-2026-68481	7.5 HIGH
CVE-2026-97791	7.5 HIGH

CWE's

CWE	Beschrijving
CWE-303	Incorrect Implementation of Authentication Algorithm
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization
CWE-404	Improper Resource Shutdown or Release
CWE-488	Exposure of Data Element to Wrong Session
CWE-672	Operation on a Resource after Expiration or Release
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-772	Missing Release of Resource after Effective Lifetime

Getroffen producten

Oracle
Commerce
Oracle Commerce 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.