Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0020

Kwetsbaarheden verholpen in Oracle Commerce

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 21-01-2026

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 kwetsbaarheden verholpen in verschillende producten, waaronder Oracle WebLogic Server en Oracle Commerce producten

Duiding

De kwetsbaarheden stellen ongeauthenticeerde aanvallers in staat om een gedeeltelijke Denial-of-Service te veroorzaken via HTTP. Dit kan leiden tot systeemuitval en verstoring van de dienstverlening. Daarnaast is er een kritieke XML External Entity (XXE) injectie kwetsbaarheid in de Apache Tika framework die de PDF-parsing functionaliteit beïnvloedt, wat kan leiden tot gevoelige informatie openbaarmaking of zelfs remote code execution.

Oplossingen

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

Referenties

- https://www.oracle.com/security-alerts/cpujan2026.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-9086	2.3 LOW
CVE-2025-41249	7.5 HIGH
CVE-2025-48924	6.5 MEDIUM
CVE-2025-50059	8.6 HIGH
CVE-2025-61795	2.3 LOW
CVE-2025-66516	10.0 CRITICAL

CWE's

CWE	Beschrijving
CWE-125	Out-of-bounds Read
CWE-201	Insertion of Sensitive Information Into Sent Data
CWE-284	Improper Access Control
CWE-285	Improper Authorization
CWE-404	Improper Resource Shutdown or Release
CWE-611	Improper Restriction of XML External Entity Reference
CWE-674	Uncontrolled Recursion
CWE-863	Incorrect Authorization
CWE-937	CWE-937
CWE-1035	CWE-1035

Getroffen producten

Oracle
Commerce
Oracle Commerce Guided Search
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.