



NCSC-2025-0329

Kwetsbaarheden verholpen in Oracle Commerce

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 23-10-2025

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 verschillende subcomponenten van Oracle Commerce producten, waaronder Oracle Middleware Common Libraries, Oracle Documaker, Oracle WebCenter Forms Recognition, Oracle WebLogic Server, en Oracle Application Testing Suite.

Duiding

De kwetsbaarheden stellen ongeauthenticeerde aanvallers in staat om gedeeltelijke of volledige Denial of Service (DoS) te veroorzaken, met CVSS-scores variërend van 2.7 tot 7.5. Dit kan leiden tot systeemuitval en ongeoorloofde toegang tot gegevens. Aanvallers kunnen deze kwetsbaarheden misbruiken door specifieke verzoeken te sturen die de systemen overbelasten of door gebruik te maken van onbetrouwbare invoer. De kwetsbaarheden zijn aangetroffen in verschillende versies van de betrokken producten, wat de impact vergroot.

Oplossingen

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

Referenties

➤ <https://www.oracle.com/docs/tech/security-alerts/cpuoct2025csaf.json>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-47554	8.7 HIGH
➤ CVE-2024-57699	5.1 MEDIUM
➤ CVE-2025-22233	2.3 LOW
➤ CVE-2025-48795	5.6 MEDIUM
➤ CVE-2025-48924	6.5 MEDIUM
➤ CVE-2025-48976	8.7 HIGH
➤ CVE-2025-48989	6.9 MEDIUM

[> CVE-2025-55163](#)**8.2 HIGH**

CWE's

CWE	Beschrijving
> CWE-20	Improper Input Validation
> CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CWE-400	Uncontrolled Resource Consumption
> CWE-404	Improper Resource Shutdown or Release
> CWE-674	Uncontrolled Recursion
> CWE-770	Allocation of Resources Without Limits or Throttling
> 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.