



NCSC-2026-0374

Kwetsbaarheden verholpen in Oracle Commerce Platform

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 16-09-2026

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 27 kwetsbaarheden verholpen in Commerce Platform, waaronder Oracle Commerce Guided Search en Oracle Commerce Experience Manager, waaronder de componenten Experience Manager, Forge en Endeca Application Controller.

Duiding

De kwetsbaarheden betreffen verschillende beveiligingsproblemen in Oracle Commerce-producten, waaronder mogelijkheden voor niet-geauthenticeerde en laaggeprivilegieerde kwaadwillenden om via netwerktoegang ongeautoriseerde acties uit te voeren. De kwetsbaarheden hebben CVSS-scores variërend van middel tot hoog. Van de in totaal 27 kwetsbaarheden kunnen volgens Oracle 16 kwetsbaarheden zonder authenticatie op afstand worden misbruikt. Succesvol misbruik kan onder meer leiden tot het verkrijgen van ongeautoriseerde toegang tot gevoelige informatie, het wijzigen van gegevens en het verstoren van de beschikbaarheid van getroffen systemen. Sommige kwetsbaarheden vereisen gebruikersinteractie of voorafgaande toegangsrechten, terwijl andere volledig op afstand en zonder authenticatie kunnen worden misbruikt.

De kwetsbaarheden met de hoogste CVSS-score van 8,2 bevinden zich in de componenten Experience Manager en Forge. Succesvolle exploitatie kan, afhankelijk van de kwetsbaarheid, een hoge impact hebben op de vertrouwelijkheid of beschikbaarheid en een beperkte impact op de integriteit van het getroffen systeem.

Het NCSC adviseert om de beveiligingsupdates met de hoogste CVSS-scores met voorrang toe te passen.

Oplossingen

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

Referenties

➤ <https://www.oracle.com/security-alerts/cspusep2026.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-83233	7.7 HIGH
➤ CVE-2026-83234	8.2 HIGH

> CVE-2026-83235	7.5 HIGH
> CVE-2026-83236	8.2 HIGH
> CVE-2026-83237	7.1 HIGH
> CVE-2026-83238	7.1 HIGH
> CVE-2026-83239	7.0 HIGH
> CVE-2026-83240	7.1 HIGH
> CVE-2026-83241	7.5 HIGH
> CVE-2026-83242	7.3 HIGH
> CVE-2026-83243	7.7 HIGH
> CVE-2026-83244	7.1 HIGH
> CVE-2026-83245	8.1 HIGH
> CVE-2026-83246	8.1 HIGH
> CVE-2026-83247	7.8 HIGH
> CVE-2026-83248	8.2 HIGH
> CVE-2026-83249	7.8 HIGH
> CVE-2026-83250	6.5 MEDIUM
> CVE-2026-83251	6.5 MEDIUM
> CVE-2026-83252	7.0 HIGH
> CVE-2026-83253	7.8 HIGH
> CVE-2026-83254	8.1 HIGH
> CVE-2026-83255	8.1 HIGH
> CVE-2026-83256	8.1 HIGH
> CVE-2026-83257	7.5 HIGH

[> CVE-2026-83258](#)

8.1 HIGH

[> CVE-2026-83259](#)

7.1 HIGH

CWE's

CWE	Beschrijving
> CWE-404	Improper Resource Shutdown or Release

Getroffen producten

Oracle
Commerce
Oracle Commerce Guided Search / Oracle Commerce Experience Manager
Oracle Corporation
Oracle Commerce Guided Search / Oracle Commerce Experience 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.