Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0255

Kwetsbaarheden verholpen in Oracle Commerce Platform

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 22-07-2026

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 39 kwetsbaarheden verholpen in Oracle Commerce Platform en Oracle Commerce Guided Search/ Experience Manager, beide versies 11.4.0.

11 van deze kwetsbaarheden hebben een CVSS score van 9 en hoger gekregen en zijn hieronder samengevat.

De overige kwetsbaarheden hebben een lagere score gekregen en detailinformatie is verder niet opgenomen in deze advisory. Hiervoor verwijst het NCSC naar de referenties.

Duiding

De kwetsbaarheden in Oracle Commerce Platform 11.4.0 stellen ongeauthenticeerde aanvallers in staat om via netwerktoegang en HTTP- of LDAP-protocollen onbevoegde toegang te verkrijgen tot gevoelige data, kritieke data te wijzigen, of volledige systeemcompromittering te veroorzaken door het uitvoeren van willekeurige code. Sommige kwetsbaarheden vereisen gebruikersinteractie, andere niet. Daarnaast kunnen aanvallers denial-of-service veroorzaken door het uitputten van systeemresources of het laten crashen van het systeem.

De Oracle Commerce Guided Search en Experience Manager modules bevatten vergelijkbare kwetsbaarheden die ongeauthenticeerde aanvallers met netwerktoegang via HTTP of RMI in staat stellen om volledige controle over het systeem te verkrijgen, gevoelige informatie te benaderen, data te manipuleren, of denial-of-service te veroorzaken. De kwetsbaarheden zijn onder meer gerelateerd aan onvoldoende toegangscontrole, authenticatieomzeiling, en onjuiste verwerking van netwerkverzoeken. De CVSS-scores van deze kwetsbaarheden variëren van 5.4 tot 9.9, waarbij meerdere kwetsbaarheden een score van 9.8 of hoger hebben, wat duidt op mogelijkheden voor volledige systeemcompromittering zonder authenticatie.

Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden in Oracle Commerce Platform en Oracle Commerce Guided Search/Experience Manager te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.oracle.com/security-alerts/cpujul2026.html
- https://www.oracle.com/security-alerts/cpujul2026verbose.html

Kwetsbaarheden

CVE	CVSS Score

CVE-2026-4176	9.8 CRITICAL
CVE-2026-61129	9.8 CRITICAL
CVE-2026-61130	9.1 CRITICAL
CVE-2026-61131	9.8 CRITICAL
CVE-2026-61145	9.8 CRITICAL
CVE-2026-61146	9.9 CRITICAL
CVE-2026-61153	9.1 CRITICAL
CVE-2026-61154	9.8 CRITICAL
CVE-2026-61155	9.1 CRITICAL
CVE-2026-61156	9.1 CRITICAL
CVE-2026-61161	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-1104	Use of Unmaintained Third Party Components
CWE-1395	Dependency on Vulnerable Third-Party Component

Getroffen producten

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

Oracle Commerce Guided Search
Platform Services

Disclaimer