Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0308

Kwetsbaarheden verholpen in Oracle Commerce Platform

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 19-08-2026

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 meerdere kwetsbaarheden verholpen in Oracle Commerce Platform versie 11.4.0

Duiding

De kwetsbaarheden ongeauthenticeerde aanvallers met netwerktoegang in staat om zonder authenticatie kritieke acties uit te voeren. Dit omvat het verkrijgen van ongeautoriseerde toegang tot gevoelige data, het wijzigen, verwijderen of creëren van kritieke gegevens, en het veroorzaken van denial-of-service (DoS) condities. Sommige kwetsbaarheden vereisen fysieke netwerktoegang of gebruikersinteractie, terwijl andere volledig op afstand en zonder authenticatie kunnen worden misbruikt.

De kwetsbaarheden kunnen leiden tot volledige systeemcompromittering, waarbij vertrouwelijkheid, integriteit en beschikbaarheid van de systemen worden aangetast. Daarnaast zijn er kwetsbaarheden die het mogelijk maken voor aanvallers met beperkte privileges of infrastructuurtoegang om hun rechten te escaleren en zo meer controle over het systeem te verkrijgen. De problemen zijn gerelateerd aan onvoldoende toegangscontrole en authenticatie binnen de getroffen componenten van de Oracle Commerce software.

Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden in Oracle Commerce Platform 11.4.0 te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.oracle.com/security-alerts/cspuaug2026.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2022-23437	6.5 MEDIUM
CVE-2024-9143	4.3 MEDIUM
CVE-2026-70953	9.8 CRITICAL
CVE-2026-70954	9.8 CRITICAL
CVE-2026-70955	7.5 HIGH

CVE-2026-70976	9.1 CRITICAL
CVE-2026-70977	9.1 CRITICAL
CVE-2026-70978	9.1 CRITICAL
CVE-2026-70979	9.1 CRITICAL
CVE-2026-70980	9.0 CRITICAL
CVE-2026-70981	9.1 CRITICAL
CVE-2026-70982	6.8 MEDIUM
CVE-2026-70983	6.8 MEDIUM
CVE-2026-70984	9.1 CRITICAL
CVE-2026-70985	7.5 HIGH
CVE-2026-70986	7.5 HIGH
CVE-2026-70987	7.5 HIGH
CVE-2026-70988	7.7 HIGH
CVE-2026-70989	6.5 MEDIUM
CVE-2026-70990	6.8 MEDIUM
CVE-2026-70991	6.3 MEDIUM
CVE-2026-70992	7.0 HIGH
CVE-2026-70993	8.2 HIGH
CVE-2026-70994	9.1 CRITICAL
CVE-2026-70995	9.8 CRITICAL
CVE-2026-70996	8.6 HIGH
CVE-2026-70997	9.1 CRITICAL
CVE-2026-70998	9.3 CRITICAL

CVE-2026-70999	8.1 HIGH
CVE-2026-71000	8.7 HIGH
CVE-2026-71001	6.5 MEDIUM
CVE-2026-71002	8.5 HIGH
CVE-2026-71003	7.1 HIGH
CVE-2026-71004	6.1 MEDIUM
CVE-2026-71005	6.1 MEDIUM
CVE-2026-71006	6.1 MEDIUM
CVE-2026-71007	6.8 MEDIUM
CVE-2026-71008	6.8 MEDIUM
CVE-2026-71009	7.4 HIGH
CVE-2026-71010	7.8 HIGH
CVE-2026-71011	6.1 MEDIUM
CVE-2026-71012	7.1 HIGH
CVE-2026-71014	9.1 CRITICAL
CVE-2026-71015	9.1 CRITICAL
CVE-2026-71016	8.2 HIGH
CVE-2026-71017	6.5 MEDIUM
CVE-2026-71018	8.2 HIGH
CVE-2026-71019	6.1 MEDIUM
CVE-2026-71020	7.6 HIGH
CVE-2026-71021	7.6 HIGH
CVE-2026-71022	7.6 HIGH

CVE-2026-71023	7.5 HIGH
CVE-2026-71024	8.2 HIGH
CVE-2026-71025	6.1 MEDIUM
CVE-2026-71026	9.1 CRITICAL
CVE-2026-71027	7.6 HIGH
CVE-2026-71028	7.8 HIGH
CVE-2026-71030	7.2 HIGH
CVE-2026-71031	6.1 MEDIUM
CVE-2026-71032	7.2 HIGH
CVE-2026-71033	5.5 MEDIUM
CVE-2026-71034	7.5 HIGH
CVE-2026-71035	8.1 HIGH
CVE-2026-71036	9.1 CRITICAL
CVE-2026-71037	9.3 CRITICAL
CVE-2026-71038	7.5 HIGH

CWE's

CWE	Beschrijving
CWE-91	XML Injection (aka Blind XPath Injection)
CWE-125	Out-of-bounds Read
CWE-787	Out-of-bounds Write
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')

Getroffen producten

Oracle
Commerce
Commerce Experience Manager
Commerce Guided Search
Commerce Platform

Disclaimer