Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0505

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Oracle E-Business Suite

Publicatiedatum: 18-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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 de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Oracle heeft 71 kwetsbaarheden verholpen in Oracle E-Business Suite, waarvan er 19 zonder authenticatie op afstand via het netwerk kunnen worden misbruikt. De kwetsbaarheden bevinden zich onder meer in Oracle Applications Framework, Oracle Application Object Library, Oracle Universal Work Queue, Oracle Mobile Field Service en Document Management and Collaboration.

Duiding

Oracle heeft zes van de 71 kwetsbaarheden als kritiek aangemerkt. Alle 6 kunnen volgens Oracle zonder authenticatie en gebruikersinteractie op afstand via het netwerk worden misbruikt. De overige kwetsbaarheden kunnen onder meer leiden tot ongeautoriseerde toegang tot gevoelige gegevens, het wijzigen of verwijderen van gegevens, het overnemen van applicatieonderdelen en verstoring van de dienstverlening.

De kwetsbaarheden met kenmerk CVE-2026-114880, CVE-2026-114924, CVE-2026-114925 en CVE-2026-114863 hebben alle vier een CVSS-score van 9.8. Een niet-geauthenticeerde kwaadwillende kan deze kwetsbaarheden via HTTP misbruiken om de betreffende Oracle E-Business Suite-componenten over te nemen. Hierdoor kunnen de vertrouwelijkheid, integriteit en beschikbaarheid van de getroffen componenten worden aangetast.

De kwetsbaarheid met kenmerk CVE-2026-101691 heeft een CVSS-score van 9.3 en kan leiden tot ongeautoriseerde toegang tot gevoelige gegevens en het wijzigen van gegevens binnen Oracle Mobile Field Service. De kwetsbaarheid met kenmerk CVE-2026-114881 heeft een CVSS-score van 9.1 en kan leiden tot het uitlezen van gevoelige gegevens en een Denial-of-Service (DoS) binnen Document Management and Collaboration.

Oracle meldt geen actief misbruik van de nieuw gepubliceerde kwetsbaarheden. Oracle vermeldt daarnaast dat de beveiligingsupdate voor de kwetsbaarheid met kenmerk CVE-2026-114918 ook de eerder actief misbruikte kwetsbaarheid CVE-2025-61882 verhelpt. Dit betreft een afzonderlijke, eerder gepubliceerde kwetsbaarheid.

De overige kwetsbaarheden variëren in ernst van gemiddeld tot hoog. Het voert te ver om iedere kwetsbaarheid afzonderlijk in detail te behandelen in deze advisory.

Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden in de genoemde versies en componenten van Oracle E-Business Suite te verhelpen. Raadpleeg My Oracle Support Note KA923 voor de benodigde beveiligingsupdates en installatie-instructies en zie bijgevoegde referentie voor meer informatie.

Referenties

- https://www.oracle.com/security-alerts/cspunov2026.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-101691	9.3 CRITICAL
CVE-2026-114863	9.8 CRITICAL
CVE-2026-114880	9.8 CRITICAL
CVE-2026-114924	9.8 CRITICAL
CVE-2026-114925	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-306	Missing Authentication for Critical Functionality

Getroffen producten

Oracle
Document Management and Collaboration
Oracle Application Object Library
Oracle Applications Framework
Oracle Mobile Field Service
Oracle Universal Work Queue

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.