



NCSC-2026-0253

Kwetsbaarheden verholpen in Oracle E-Business Suite componenten

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 meerdere kwetsbaarheden verholpen in Oracle E-Business Suite, inclusief diverse modules zoals Work in Process, Application Object Library, HRMS, Applications Framework, Advanced Collections, Advanced Outbound Telephony, Advanced Pricing, Applications DBA, Bills of Material, Customer Care, Enterprise Asset Management, Enterprise Command Center Framework, Flow Manufacturing, General Ledger, Installed Base, iReceivables, Labor Distribution, Order Management, Payables, Payroll, Process Manufacturing, Product Hub, Project Intelligence, Public Sector Financials, Sales Offline, SDP Number Portability, Trade Management, Transportation Execution, Warehouse Management, Yard Management, TeleSales, Service Fulfillment Manager, Contracts Integration, Applications Manager, Common Application Components, Price Protection, Workflow, en andere componenten binnen de versies 12.2.3 tot en met 12.2.15.

Het totaal aantal kwetsbaarheden dat is verholpen in deze updates is 410.

Duiding

De ernstigste kwetsbaarheden, 4 stuks, hebben een hoge score variërend van 9.1 tot 9.8 gekregen en bevinden zich in diverse Oracle E-Business componenten. De kwetsbaarheid met de score van 9.8 stelt ongeauthenticeerde aanvallers in staat om via HTTP het Oracle Work in Process over te nemen. Een beperkende factor is dat de kwetsbare producten niet ontworpen zijn om publiek toegankelijk te zijn. Hierdoor is de kans op grootschalig misbruik kleiner.

De overige ernstige kwetsbaarheden kunnen, afhankelijk van de vereiste rechten, via HTTP of HTTPS worden misbruikt, waardoor een aanvaller ongeautoriseerde toegang kan verkrijgen tot gevoelige gegevens, deze kan wijzigen of verwijderen, of zelfs volledige controle kan krijgen over onderdelen van de Oracle Applications Framework-omgeving.

De overige 406 kwetsbaarheden hebben lagere scores gekregen dan 9. De detailinformatie voor deze kwetsbaarheden is niet opgenomen in deze advisory en het NCSC verwijst daarom naar de bijgevoegde referentie.

Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden in de genoemde componenten van Oracle E-Business Suite 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-2026-60880	9.8 CRITICAL
> CVE-2026-60773	9.6 CRITICAL
> CVE-2026-62549	5.3 MEDIUM
> CVE-2026-62546	9.1 CRITICAL

CWE's

CWE	Beschrijving
> CWE-184	Incomplete List of Disallowed Inputs
> CWE-269	Improper Privilege Management
> CWE-285	Improper Authorization

Getroffen producten

Oracle
E-Business Suite
HRMS
Oracle Application Object Library
Oracle Applications Framework
Oracle Corporation
Oracle HRMS (UK)

Oracle Work in
Process

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.