



# NCSC-2026-0170

## Kwetsbaarheden verholpen in Oracle E-Business Suite componenten

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 29-05-2026

### **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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Feiten

Oracle heeft kwetsbaarheden verholpen in verschillende componenten van Oracle E-Business Suite, waaronder Oracle Payments, Oracle Internet Procurement Connector, Oracle Financials Common Modules, Oracle iAssets, Oracle Public Sector Financials (International), Oracle Universal Work Queue, Oracle Payroll en Oracle Flow Manufacturing, specifiek in versies 12.2.3 tot en met 12.2.15.

## Duiding

De kwetsbaarheden maken het mogelijk voor een aanvaller, vaak met lage privileges en via netwerktoegang over HTTP of HTTPS, om kritieke acties uit te voeren zoals het verkrijgen van volledige systeemcompromittatie, het creëren, verwijderen of wijzigen van belangrijke data, en het uitvoeren van SQL-injecties. Sommige kwetsbaarheden stellen een aanvaller in staat om volledige controle over het systeem te verkrijgen, terwijl andere leiden tot ongeautoriseerde toegang en manipulatie van gevoelige gegevens. De kwetsbaarheden zijn aanwezig in verschillende Oracle-producten binnen de genoemde versies en kunnen leiden tot compromittering van vertrouwelijkheid, integriteit en beschikbaarheid van systemen en data.

## 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/cspumay2026.html>

## Kwetsbaarheden

CVE	CVSS Score
➤ <a href="#">CVE-2026-46817</a>	9.8 CRITICAL
➤ <a href="#">CVE-2026-46818</a>	7.4 HIGH
➤ <a href="#">CVE-2026-46819</a>	9.1 CRITICAL
➤ <a href="#">CVE-2026-46820</a>	8.5 HIGH
➤ <a href="#">CVE-2026-46821</a>	7.7 HIGH

> CVE-2026-46822	9.9 CRITICAL
> CVE-2026-46823	7.7 HIGH
> CVE-2026-46824	9.9 CRITICAL
> CVE-2026-46826	8.8 HIGH
> CVE-2026-46827	8.8 HIGH
> CVE-2026-46828	8.1 HIGH
> CVE-2026-46837	8.8 HIGH

## CWE's

CWE	Beschrijving
> CVE-190	Integer Overflow or Wraparound
> CVE-94	Improper Control of Generation of Code ('Code Injection')
> CVE-125	Out-of-bounds Read
> CVE-522	Insufficiently Protected Credentials
> CVE-1287	Improper Validation of Specified Type of Input
> CVE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
> CVE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

## Getroffen producten

<b>Oracle</b>
E-Business Suite
Oracle Universal Work Queue

<b>Oracle Corporation</b>
Oracle Financials Common Modules
Oracle Flow Manufacturing
Oracle Internet Procurement Connector
Oracle Payments
Oracle Payroll
Oracle Public Sector Financials (International)
Oracle iAssets

## 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 or 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.