



NCSC-2026-0206

Kwetsbaarheden verholpen in Oracle JD Edwards EnterpriseOne

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 17-06-2026

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 JD Edwards EnterpriseOne, inclusief de modules Tools, Accounts Payable, Human Resources Management, General Ledger, Order Promising en Project Costing, specifiek voor versies 9.2.0.0 tot en met 9.2.26.2.

Duiding

De kwetsbaarheden in Oracle JD Edwards EnterpriseOne stellen een aanvaller in staat om zonder authenticatie of met lage privileges via netwerktoegang (HTTP of SMB) volledige controle over het systeem te verkrijgen. Dit omvat het creëren, verwijderen of wijzigen van kritieke data, het verkrijgen van ongeautoriseerde toegang tot gevoelige informatie, en het veroorzaken van een denial-of-service door het systeem te laten crashen. De kwetsbaarheden beïnvloeden de vertrouwelijkheid, integriteit en beschikbaarheid van het systeem. Sommige kwetsbaarheden kunnen ook impact hebben op andere gerelateerde Oracle-producten vanwege de geïntegreerde aard van de suite.

Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden in JD Edwards EnterpriseOne en de gerelateerde modules te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://www.oracle.com/security-alerts/cspujun2026.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-46878	9.3 CRITICAL
➤ CVE-2026-46879	9.3 CRITICAL
➤ CVE-2026-46880	9.3 CRITICAL
➤ CVE-2026-46881	9.3 CRITICAL
➤ CVE-2026-46882	9.3 CRITICAL
➤ CVE-2026-46883	9.3 CRITICAL

➤ CVE-2026-46891	5.3 MEDIUM
➤ CVE-2026-46892	9.1 CRITICAL
➤ CVE-2026-46893	8.7 HIGH
➤ CVE-2026-46903	8.8 HIGH
➤ CVE-2026-46904	9.3 CRITICAL
➤ CVE-2026-46905	9.8 CRITICAL
➤ CVE-2026-46906	5.3 MEDIUM
➤ CVE-2026-46907	9.9 CRITICAL
➤ CVE-2026-46908	9.9 CRITICAL
➤ CVE-2026-46909	9.8 CRITICAL
➤ CVE-2026-46910	6.9 MEDIUM
➤ CVE-2026-46911	5.3 MEDIUM
➤ CVE-2026-46912	6.9 MEDIUM
➤ CVE-2026-46913	8.5 HIGH

CWE's

CWE	Beschrijving
➤ CVE-285	Improper Authorization

Getroffen producten

Oracle
JD Edwards EnterpriseOne Accounts Payable

JD Edwards EnterpriseOne General Ledger
JD Edwards EnterpriseOne Human Resources Management
JD Edwards EnterpriseOne Order Promising
JD Edwards EnterpriseOne Project Costing
JD Edwards EnterpriseOne Tools

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.