



NCSC-2025-0131

Kwetsbaarheden verholpen in Oracle JD Edwards

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 16-04-2025

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 kwetsbaarheden verholpen in JD Edwards EnterpriseOne Tools (Specifiek voor versies 9.2.0.0 tot 9.2.9.2).

Duiding

De kwetsbaarheden in JD Edwards EnterpriseOne Tools stellen ongeauthenteerde kwaadwillenden in staat om via HTTP toegang te krijgen tot het systeem, wat kan leiden tot ongeautoriseerde toegang tot gevoelige gegevens en manipulatie daarvan of zelfs volledige overname van JD Edwards EnterpriseOne Tools. Enkele van de kwetsbaarheden kunnen leiden tot gedeeltelijke of volledige DoS, hiervoor is echter wel gebruikersinteractie vereist.

Oplossingen

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

Referenties

➤ <https://www.oracle.com/security-alerts/cpuapr2025.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-5535	9.1 CRITICAL
➤ CVE-2024-23807	9.8 CRITICAL
➤ CVE-2024-25710	8.1 HIGH
➤ CVE-2024-45613	6.9 MEDIUM
➤ CVE-2024-47554	8.7 HIGH
➤ CVE-2025-21586	5.4 MEDIUM
➤ CVE-2025-30709	6.1 MEDIUM
➤ CVE-2025-30740	6.5 MEDIUM

CWE's

CWE	Beschrijving
> CWE-1395	Dependency on Vulnerable Third-Party Component
> CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
> CWE-416	Use After Free
> CWE-400	Uncontrolled Resource Consumption
> CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')
> CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

Oracle
JD Edwards
JD Edwards EnterpriseOne Tools
Jd Edwards Enterpriseone Tools
Oracle Corporation
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.