



Advisory NCSC-2026-0446

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Oracle JD Edwards EnterpriseOne

Publicatiedatum: 22-10-2026

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 delen. 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 meerdere kwetsbaarheden verholpen in Oracle JD Edwards EnterpriseOne Tools, specifiek in versies 9.2.0.0 tot en met 9.2.26.5.

Duiding

De kwetsbaarheden in Oracle JD Edwards EnterpriseOne Tools stellen een aanvaller in staat om via verschillende netwerkprotocollen zoals HTTP, HTTPS, SMTP zonder authenticatie of met lage privileges toegang te verkrijgen tot het systeem. Hierdoor kan een aanvaller data creëren, wijzigen of verwijderen, en in sommige gevallen volledige controle over het systeem verkrijgen. Sommige kwetsbaarheden vereisen gebruikersinteractie, andere niet. De impact betreft de vertrouwelijkheid, integriteit en beschikbaarheid van het systeem en de data.

Oplossingen

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

Referenties

- <https://www.oracle.com/security-alerts/cpuoct2026.html>

Kwetsbaarheden

CVE	CVSS Score
CVE-2022-45378	9.8 CRITICAL
CVE-2025-15467	9.8 CRITICAL
CVE-2026-87305	8.1 HIGH
CVE-2026-87306	8.1 HIGH
CVE-2026-87309	8.1 HIGH
CVE-2026-87310	8.8 HIGH

CVE	CVSS Score
CVE-2026-87313	8.8 HIGH
CVE-2026-91265	9.1 CRITICAL
CVE-2026-91266	8.4 HIGH
CVE-2026-91267	8.6 HIGH
CVE-2026-91268	8.8 HIGH
CVE-2026-91269	8.1 HIGH
CVE-2026-91270	8.8 HIGH
CVE-2026-91271	8.1 HIGH
CVE-2026-91273	8.6 HIGH
CVE-2026-91286	8.2 HIGH
CVE-2026-91287	8.1 HIGH
CVE-2026-91295	8.8 HIGH
CVE-2026-91296	8.8 HIGH
CVE-2026-91303	8.8 HIGH
CVE-2026-91305	9.1 CRITICAL
CVE-2026-91310	8.8 HIGH
CVE-2026-91313	8.1 HIGH
CVE-2026-91326	8.8 HIGH

CWE's

CWE	Beschrijving
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-306	Missing Authentication for Critical Function
CWE-502	Deserialization of Untrusted Data
CWE-787	Out-of-bounds Write

Getroffen producten

Oracle
JD Edwards
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 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.