



NCSC-2025-0033

Kwetsbaarheden verholpen in Oracle E-Business Suite

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 28-01-2025

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 Oracle E-Business Suite (Specifiek voor de Advanced Outbound Telephony, Project Foundation, Customer Care en Workflow componenten).

Duiding

De kwetsbaarheden bevinden zich in verschillende componenten van de Oracle E-Business Suite. De Advanced Outbound Telephony component bevat een kwetsbaarheid die ongeauthenticeerde kwaadwillenden in staat stelt om het systeem te compromitteren, wat kan leiden tot ongeautoriseerde toegang tot gevoelige gegevens en wijzigingen. De Project Foundation component laat laaggeprivilegieerde kwaadwillenden met netwerktoegang toe om ongeautoriseerde creatie, verwijdering, wijziging en toegang tot gegevens te realiseren. De Customer Care component kan worden misbruikt door laaggeprivilegieerde kwaadwillenden via HTTP-verzoeken, wat kan resulteren in ongeautoriseerde toegang en wijziging van gevoelige gegevens. De Workflow component heeft ook een kwetsbaarheid die kan worden geëxploiteerd door laaggeprivilegieerde kwaadwillenden via HTTP-verzoeken, wat kan leiden tot ongeautoriseerde toegang en wijzigingen van gevoelige gegevens.

Oplossingen

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

Referenties

➤ <https://www.oracle.com/security-alerts/cpujan2025.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-21489	6.1 MEDIUM
➤ CVE-2025-21506	8.1 HIGH
➤ CVE-2025-21516	8.1 HIGH
➤ CVE-2025-21541	5.4 MEDIUM

CWE's

CWE	Beschrijving
➤ CWE-281	Improper Preservation of Permissions
➤ CWE-352	Cross-Site Request Forgery (CSRF)
➤ CWE-863	Incorrect Authorization

Getroffen producten

oracle
advanced_outbound_telephony
customer_care
project_foundation
workflow

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.