



Advisory NCSC-2026-0442

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Oracle E-Business Suite

Publicatiedatum: 21-10-2026

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 194 kwetsbaarheden verholpen in Oracle E-Business Suite en gerelateerde componenten, specifiek voor versies 12.2.3 tot en met 12.2.15.

Duiding

Afhankelijk van de specifieke kwetsbaarheid kunnen deze door een aanvaller met netwerktoegang worden misbruikt om ongeautoriseerde toegang tot gegevens te verkrijgen of om gegevens aan te maken, in te zien, te wijzigen of te verwijderen. In ernstige gevallen kan misbruik leiden tot Remote Code Execution (RCE), waardoor een aanvaller willekeurige code kan uitvoeren op het getroffen systeem.

Een deel van de kwetsbaarheden kan op afstand worden misbruikt zonder authenticatie. Voor andere kwetsbaarheden zijn geldige inloggegevens, specifieke toegangsrechten of gebruikersinteractie vereist. De impact en de voorwaarden voor misbruik verschillen per kwetsbaarheid en getroffen component. De CVSS 3.1-scores lopen op tot de maximale score van 10,0.

Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden in de genoemde versies en componenten van Oracle E-Business Suite te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

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

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-83361	8.1 HIGH
CVE-2026-83363	8.8 HIGH
CVE-2026-83393	8.5 HIGH
CVE-2026-87408	8.7 HIGH

CVE	CVSS Score
CVE-2026-91347	8.5 HIGH
CVE-2026-91506	8.1 HIGH
CVE-2026-91532	8.8 HIGH
CVE-2026-101534	8.5 HIGH
CVE-2026-101542	8.8 HIGH
CVE-2026-101557	8.8 HIGH
CVE-2026-101567	8.8 HIGH
CVE-2026-101634	9.1 CRITICAL
CVE-2026-101635	8.8 HIGH
CVE-2026-101640	8.2 HIGH
CVE-2026-101648	8.4 HIGH
CVE-2026-101653	8.8 HIGH
CVE-2026-101654	8.8 HIGH
CVE-2026-101655	8.8 HIGH
CVE-2026-101656	8.8 HIGH
CVE-2026-101664	8.8 HIGH
CVE-2026-101665	8.1 HIGH
CVE-2026-101672	8.1 HIGH
CVE-2026-101684	8.3 HIGH
CVE-2026-101685	8.8 HIGH
CVE-2026-101686	8.8 HIGH
CVE-2026-101688	8.6 HIGH
CVE-2026-101690	8.2 HIGH
CVE-2026-101692	8.8 HIGH
CVE-2026-101700	8.1 HIGH
CVE-2026-101704	8.2 HIGH
CVE-2026-101742	8.8 HIGH
CVE-2026-101767	9.8 CRITICAL
CVE-2026-101808	9.1 CRITICAL
CVE-2026-101809	10.0 CRITICAL
CVE-2026-101813	8.8 HIGH

CVE	CVSS Score
CVE-2026-101824	8.7 HIGH
CVE-2026-101831	8.1 HIGH
CVE-2026-101834	8.1 HIGH
CVE-2026-101841	8.2 HIGH
CVE-2026-101842	8.8 HIGH
CVE-2026-101852	8.8 HIGH
CVE-2026-101853	8.8 HIGH
CVE-2026-101854	8.8 HIGH

CWE's

CWE	Beschrijving
CWE-306	Missing Authentication for Critical Function

Getroffen producten

Oracle
E-Business Suite

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.