



NCSC-2026-0381

Kwetsbaarheden verholpen in Oracle PeopleSoft Enterprise

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 16-09-2026

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 16 kwetsbaarheden verholpen in diverse Oracle PeopleSoft-producten, waaronder PeopleSoft Enterprise PeopleTools, PeopleSoft Enterprise PRTL Interaction Hub en PeopleSoft Enterprise CC Common Application Objects.

Duiding

De kwetsbaarheden betreffen verschillende beveiligingsproblemen in Oracle PeopleSoft-producten, waaronder mogelijkheden voor niet-geauthenticeerde en laaggeprivilegieerde kwaadwillenden om via netwerktoegang ongeautoriseerde acties uit te voeren. De kwetsbaarheden hebben CVSS-scores in de categorie hoog. Van de in totaal 16 kwetsbaarheden kunnen volgens Oracle vier kwetsbaarheden zonder authenticatie op afstand worden misbruikt. Succesvol misbruik kan onder meer leiden tot het verkrijgen van ongeautoriseerde toegang tot gevoelige informatie, het wijzigen van gegevens, volledige overname van getroffen componenten en het verstoren van de beschikbaarheid van getroffen systemen. Sommige kwetsbaarheden vereisen gebruikersinteractie of voorafgaande toegangsrechten, terwijl andere volledig op afstand en zonder authenticatie kunnen worden misbruikt.

Geen van de kwetsbaarheden is als kritiek aangemerkt. CVE-2026-83017 heeft met een CVSS-score van 8,8 de hoogste score en bevindt zich in de Report Distribution-component van PeopleSoft Enterprise PeopleTools. Voor misbruik is een laaggeprivilegieerd account vereist. CVE-2026-73954 heeft een CVSS-score van 8,1 en bevindt zich in de Business Interlink-component van PeopleSoft Enterprise PeopleTools. Deze kwetsbaarheid kan zonder authenticatie op afstand via HTTP worden misbruikt en kan volgens Oracle leiden tot volledige overname van PeopleSoft Enterprise PeopleTools. Oracle kwalificeert de kwetsbaarheid echter als moeilijk te misbruiken.

Oplossingen

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

Referenties

➤ <https://www.oracle.com/security-alerts/cspusep2026.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-7598	6.9 MEDIUM

> CVE-2026-25639	7.5 HIGH
> CVE-2026-73954	8.1 HIGH
> CVE-2026-73955	7.3 HIGH
> CVE-2026-73960	7.5 HIGH
> CVE-2026-82993	8.5 HIGH
> CVE-2026-83014	8.1 HIGH
> CVE-2026-83015	7.0 HIGH
> CVE-2026-83016	7.2 HIGH
> CVE-2026-83017	8.8 HIGH
> CVE-2026-83018	7.8 HIGH
> CVE-2026-83019	8.1 HIGH
> CVE-2026-83070	7.7 HIGH
> CVE-2026-87264	7.7 HIGH

CWE's

CWE	Beschrijving
> CVE-190	Integer Overflow or Wraparound
> CVE-754	Improper Check for Unusual or Exceptional Conditions
> CVE-1287	Improper Validation of Specified Type of Input
> CVE-1321	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')

Getroffen producten

Oracle
PeopleSoft
PeopleSoft Enterprise PeopleTools

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.