



# NCSC-2026-0204

## Kwetsbaarheden verholpen in Oracle PeopleSoft Enterprise

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 17-06-2026

### **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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Feiten

Oracle heeft kwetsbaarheden verholpen in Oracle PeopleSoft Enterprise PT PeopleTools (versies 8.61 en 8.62) en PeopleSoft Enterprise CS Campus Community en Student Financials (versie 9.2.38).

## Duiding

De kwetsbaarheden in Oracle PeopleSoft Enterprise PT PeopleTools versies 8.61 en 8.62 stellen ongeauthenticeerde aanvallers met netwerktoegang via HTTP of HTTPS in staat om authenticatiecontroles te omzeilen, waardoor zij kritieke data kunnen creëren, verwijderen of wijzigen. Sommige kwetsbaarheden maken het mogelijk om volledige systeemcompromittering te bereiken, inclusief het uitvoeren van willekeurige code en het overnemen van het systeem. Daarnaast kunnen aanvallers met hoge privileges en infrastructuurtoegang volledige controle over het systeem verkrijgen. De kwetsbaarheden beïnvloeden de vertrouwelijkheid, integriteit en beschikbaarheid van het systeem. Voor PeopleSoft Enterprise CS Campus Community en Student Financials versie 9.2.38 kunnen aanvallers met lage of hoge privileges en netwerktoegang via HTTP of HTTPS eveneens kritieke data manipuleren of het systeem overnemen. De kwetsbaarheden zijn gerelateerd aan onvoldoende toegangscontrole en beïnvloeden belangrijke componenten van de PeopleSoft-omgeving.

## Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden in PeopleSoft Enterprise PT PeopleTools en PeopleSoft Enterprise CS Campus Community en Student Financials te verhelpen. Zie bijgevoegde referenties voor meer informatie.

## Referenties

➤ <https://www.oracle.com/security-alerts/cspujun2026.html>

## Kwetsbaarheden

CVE	CVSS Score
➤ <a href="#">CVE-2026-35271</a>	8.7 HIGH
➤ <a href="#">CVE-2026-35272</a>	8.4 HIGH
➤ <a href="#">CVE-2026-35274</a>	8.2 HIGH
➤ <a href="#">CVE-2026-35276</a>	8.1 HIGH

> CVE-2026-35278	9.8 CRITICAL
> CVE-2026-35279	8.1 HIGH
> CVE-2026-35288	8.2 HIGH
> CVE-2026-35289	8.1 HIGH
> CVE-2026-46849	8.1 HIGH
> CVE-2026-46851	8.1 HIGH
> CVE-2026-46979	5.1 MEDIUM

### CWE's

CWE	Beschrijving
> CVE-285	Improper Authorization

### Getroffen producten

<b>Oracle</b>
PeopleSoft Enterprise CS Campus Community
PeopleSoft Enterprise CS Student Financials
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.