Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0504

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Oracle PeopleSoft Enterprise

Publicatiedatum: 18-11-2026

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 de-len. 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 PeopleSoft Enterprise PeopleTools en gerelateerde componenten, waaronder Application Server, Integration Broker en Report Distribution, specifiek in versies 8.61 tot en met 8.63.

Duiding

De kwetsbaarheden in Oracle PeopleSoft Enterprise PeopleTools en de gerelateerde componenten stellen een aanvaller in staat om via HTTP-netwerktoegang zonder of met beperkte privileges acties uit te voeren die kunnen leiden tot ongeautoriseerde toegang, het omzeilen van authenticatie, het wijzigen, verwijderen of creëren van kritieke data, en in sommige gevallen volledige overname van het systeem. De kwetsbaarheden beïnvloeden vertrouwelijkheid, integriteit en beschikbaarheid van het systeem. Oracle Outside In Technology versie 8.5.8 is kwetsbaar voor denial of service via HTTP, wat frequente crashes veroorzaakt. De genoemde kwetsbaarheden zijn exploiteerbaar via netwerktoegang en sommige vereisen geen authenticatie.

Oplossingen

Oracle heeft updates uitgebracht voor PeopleSoft Enterprise PeopleTools en de gerelateerde componenten om de kwetsbaarheden te verhelpen.

Referenties

- https://www.oracle.com/security-alerts/cspunov2026.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-111497	9.2 CRITICAL
CVE-2026-114862	9.1 CRITICAL
CVE-2026-114928	8.8 HIGH
CVE-2026-114937	8.8 HIGH

CVE	CVSS Score
CVE-2024-41311	8.8 HIGH
CVE-2026-114932	8.7 HIGH
CVE-2026-114933	8.2 HIGH
CVE-2026-114931	7.8 HIGH
CVE-2026-114929	7.5 HIGH
CVE-2026-114930	7.5 HIGH
CVE-2026-114935	7.5 HIGH
CVE-2026-114927	7.2 HIGH

CWE's

CWE	Beschrijving
CWE-125	Out-of-bounds Read
CWE-252	Unchecked Return Value
CWE-295	Improper Certificate Validation
CWE-306	Missing Authentication for Critical Functionality
CWE-787	Out-of-bounds Write

Getroffen producten

Oracle
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.