



Advisory NCSC-2026-0439

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Oracle PeopleSoft Enterprise

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 nieuwe kwetsbaarheden verholpen in Oracle PeopleSoft Enterprise.

Duiding

De kwetsbaarheden in Oracle PeopleSoft Enterprise betreffen verschillende beveiligingsrisico's, waaronder ongeautoriseerde toegang tot gegevens, ongeautoriseerde wijzigingen van gegevens en verstoring van de beschikbaarheid van systemen (denial-of-service, DoS). Afhankelijk van de specifieke kwetsbaarheid kan misbruik leiden tot aantasting van de vertrouwelijkheid, integriteit of beschikbaarheid van gegevens en systemen. Sommige kwetsbaarheden zijn via het netwerk exploiteerbaar en vereisen geen authenticatie, terwijl andere lokale toegang, authenticatie of aanvullende voorwaarden vereisen. De kwetsbaarheden treffen diverse componenten van Oracle PeopleTools en andere PeopleSoft Enterprise-modules. De ernst en potentiële impact verschillen per kwetsbaarheid; de daadwerkelijke gevolgen zijn afhankelijk van de getroffen component, de configuratie en de voorwaarden voor exploitatie.

Oplossingen

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

Referenties

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

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-20925	4.3 MEDIUM
CVE-2026-9076	7.5 HIGH
CVE-2026-9563	7.5 HIGH
CVE-2026-12816	8.7 HIGH

CVE	CVSS Score
CVE-2026-33466	9.8 CRITICAL
CVE-2026-55200	9.2 CRITICAL
CVE-2026-60500	5.8 MEDIUM
CVE-2026-60743	6.5 MEDIUM
CVE-2026-60745	4.4 MEDIUM
CVE-2026-60809	4.2 MEDIUM
CVE-2026-60814	3.9 LOW
CVE-2026-60819	3.7 LOW
CVE-2026-60839	5.5 MEDIUM
CVE-2026-60869	6.8 MEDIUM
CVE-2026-60874	4.2 MEDIUM
CVE-2026-60876	4.2 MEDIUM
CVE-2026-60878	4.4 MEDIUM
CVE-2026-60881	6.5 MEDIUM
CVE-2026-60882	5.3 MEDIUM
CVE-2026-60885	6.8 MEDIUM
CVE-2026-60887	3.8 LOW
CVE-2026-60964	1.9 LOW
CVE-2026-60968	6.0 MEDIUM
CVE-2026-70860	5.9 MEDIUM
CVE-2026-70869	4.7 MEDIUM
CVE-2026-83372	5.4 MEDIUM
CVE-2026-83373	3.0 LOW
CVE-2026-83375	6.0 MEDIUM
CVE-2026-83427	6.6 MEDIUM
CVE-2026-87336	5.3 MEDIUM
CVE-2026-87340	3.7 LOW
CVE-2026-87342	6.5 MEDIUM
CVE-2026-87343	4.8 MEDIUM
CVE-2026-87344	6.5 MEDIUM
CVE-2026-87345	6.1 MEDIUM

CVE	CVSS Score
CVE-2026-87348	4.2 MEDIUM
CVE-2026-87349	6.5 MEDIUM
CVE-2026-87350	4.5 MEDIUM
CVE-2026-87352	4.4 MEDIUM
CVE-2026-87353	4.5 MEDIUM
CVE-2026-87355	4.4 MEDIUM
CVE-2026-87401	3.3 LOW
CVE-2026-87409	6.5 MEDIUM
CVE-2026-87410	6.8 MEDIUM
CVE-2026-87412	2.7 LOW
CVE-2026-87415	5.3 MEDIUM
CVE-2026-87416	3.7 LOW
CVE-2026-87418	2.5 LOW
CVE-2026-91263	4.9 MEDIUM
CVE-2026-91264	3.7 LOW
CVE-2026-91331	3.8 LOW
CVE-2026-91356	4.2 MEDIUM
CVE-2026-91465	7.5 HIGH
CVE-2026-91466	6.4 MEDIUM
CVE-2026-91468	6.5 MEDIUM
CVE-2026-91471	3.7 LOW
CVE-2026-91474	6.1 MEDIUM
CVE-2026-91476	5.3 MEDIUM
CVE-2026-91478	8.8 HIGH
CVE-2026-91480	6.5 MEDIUM
CVE-2026-91481	5.4 MEDIUM
CVE-2026-91482	6.5 MEDIUM
CVE-2026-91485	3.8 LOW
CVE-2026-91486	4.4 MEDIUM
CVE-2026-91497	5.3 MEDIUM
CVE-2026-91505	6.0 MEDIUM

CVE	CVSS Score
CVE-2026-91519	6.5 MEDIUM
CVE-2026-91541	6.5 MEDIUM
CVE-2026-91553	4.4 MEDIUM
CVE-2026-91559	4.4 MEDIUM
CVE-2026-91562	4.4 MEDIUM
CVE-2026-101388	7.1 HIGH
CVE-2026-101389	5.9 MEDIUM
CVE-2026-101390	8.1 HIGH
CVE-2026-101407	5.5 MEDIUM
CVE-2026-101409	7.5 HIGH
CVE-2026-101410	7.5 HIGH
CVE-2026-101411	8.1 HIGH
CVE-2026-101412	5.8 MEDIUM
CVE-2026-101413	5.3 MEDIUM
CVE-2026-101414	2.9 LOW
CVE-2026-101415	3.1 LOW
CVE-2026-101416	7.5 HIGH
CVE-2026-101417	3.7 LOW
CVE-2026-101418	6.5 MEDIUM
CVE-2026-101419	6.5 MEDIUM
CVE-2026-101420	9.6 CRITICAL
CVE-2026-101421	7.5 HIGH
CVE-2026-101422	8.1 HIGH
CVE-2026-101423	4.3 MEDIUM
CVE-2026-101424	5.8 MEDIUM
CVE-2026-101425	2.5 LOW
CVE-2026-101426	6.9 MEDIUM
CVE-2026-101427	8.1 HIGH
CVE-2026-101428	7.5 HIGH
CVE-2026-101429	7.0 HIGH
CVE-2026-101430	6.2 MEDIUM

CVE	CVSS Score
CVE-2026-101431	8.7 HIGH
CVE-2026-101432	5.3 MEDIUM
CVE-2026-101433	5.3 MEDIUM
CVE-2026-101434	7.6 HIGH
CVE-2026-101435	6.6 MEDIUM
CVE-2026-101450	7.1 HIGH
CVE-2026-101486	5.4 MEDIUM
CVE-2026-101487	5.4 MEDIUM
CVE-2026-101488	6.5 MEDIUM
CVE-2026-101489	4.3 MEDIUM
CVE-2026-101490	6.1 MEDIUM
CVE-2026-101491	5.0 MEDIUM

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-131	Incorrect Calculation of Buffer Size
CWE-125	Out-of-bounds Read
CWE-347	Improper Verification of Cryptographic Signature
CWE-354	Improper Validation of Integrity Check Value
CWE-770	Allocation of Resources Without Limits or Throttling

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 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.