Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0260

Kwetsbaarheden verholpen in Oracle PeopleSoft Enterprise

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 22-07-2026

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 84 kwetsbaarheden verholpen in verschillende modules van Oracle PeopleSoft Enterprise, waaronder HCM Talent Acquisition Manager, In-Memory Project Discovery, FIN Expenses, SCM eProcurement, CC Common Application Objects, SCM Order Management, CRM Common Objects en FIN Program Management, allen versie 9.2.

Een deel van deze 84 kwetsbaarheden betreft objecten die belangrijk zijn voor andere landen en zijn dus niet relevant voor sytemen in Nederland.

Duiding

De ernstigste kwetsbaarheden, 8 stuks, hebben een hoge score variërend van 9.1 tot 9.9 gekregen en bevinden zich in diverse Oracle PeopleSoft Enterprise componenten.

De twee meest ernstige kwetsbaarheden in HCM Talent Acquisition Manager en Project Discovery, met de score van 9.9 maken het mogelijk voor een aanvaller met lage privileges en netwerktoegang via HTTP om het systeem volledig te compromitteren. Hierdoor kan de aanvaller de vertrouwelijkheid, integriteit en beschikbaarheid van de omgeving beïnvloeden. De kwetsbaarheid kan ook impact hebben op andere Oracle-producten buiten de Talent Acquisition Manager module.

De kwetsbaarheid in Enterprise FIN Expenses, met de score van 9.4 maakt het mogelijk voor niet-geauthenticeerde externe aanvallers om ongeautoriseerde toegang te verkrijgen tot het systeem. Door misbruik van deze kwetsbaarheid kunnen aanvallers data binnen de applicatie wijzigen of verwijderen. Daarnaast kan de kwetsbaarheid worden gebruikt om een gedeeltelijke denial-of-service (DoS) te veroorzaken.

De kwetsbaarheid in SCM eProcurement, met de score 9.3 maakt het mogelijk voor ongeauthenticeerde aanvallers met netwerktoegang via HTTP om ongeautoriseerde toegang tot het systeem te verkrijgen. Door misbruik van deze kwetsbaarheid kan een aanvaller kritieke gegevens binnen de getroffen applicatie wijzigen. De kwetsbaarheid kan ook invloed hebben op andere gerelateerde Oracle PeopleSoft producten.

De kwetsbaarheid in Common Application Objects, met de score 9.1 maakt het mogelijk voor ongeauthenticeerde aanvallers met netwerktoegang via HTTP om onbevoegd kritieke data te creëren, verwijderen of wijzigen. Dit betreft de Common Application Objects component binnen de PeopleSoft Enterprise suite. Aanvallers kunnen hierdoor gevoelige data manipuleren zonder authenticatie.

De kwetsbaarheid in SCM Order Management, met de score 9.1 maakt het mogelijk voor ongeauthenticeerde aanvallers met netwerktoegang via HTTP om onbevoegd kritieke data te creëren, verwijderen of wijzigen. Dit betreft de Common Application Objects component binnen de PeopleSoft Enterprise suite. Aanvallers kunnen hierdoor gevoelige data manipuleren zonder authenticatie.

De kwetsbaarheid in Enterprise CRM Common Objects, met score 9.0 maakt het mogelijk voor ongeauthenticeerde aanvallers met netwerktoegang via HTTP om onbevoegd kritieke data te creëren,

verwijderen of wijzigen. Dit betreft de Common Application Objects component binnen de PeopleSoft Enterprise suite. Aanvallers kunnen hierdoor gevoelige data manipuleren zonder authenticatie.

De kwetsbaarheid in Program Management, met score 9.0 maakt het mogelijk voor een aanvaller met beperkte rechten en netwerktoegang, en die gebruikersinteractie vereist, om mogelijk volledige controle over het getroffen systeem te verkrijgen. De kwetsbaarheid beïnvloedt de vertrouwelijkheid, integriteit en beschikbaarheid van het systeem.

De overige kwetsbaarheden hebben lagere scores gekregen dan 9. Deze kunnen leiden tot compromittering van vertrouwelijkheid, integriteit en beschikbaarheid van de systemen. Sommige kwetsbaarheden vereisen gebruikersinteractie, terwijl andere dat niet doen. De impact strekt zich uit over meerdere modules binnen de PeopleSoft Enterprise suite en kan ook andere gerelateerde Oracle producten beïnvloeden.

De detailinformatie voor deze kwetsbaarheden is niet opgenomen in deze advisory en het NCSC verwijst daarom naar de bijgevoegde referentie.

Oplossingen

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

Referenties

- https://www.oracle.com/security-alerts/cpujul2026.html
- https://www.oracle.com/security-alerts/cpujul2026verbose.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-61076	9.9 CRITICAL
CVE-2026-61209	9.9 CRITICAL
CVE-2026-61203	9.4 CRITICAL
CVE-2026-61207	9.3 CRITICAL
CVE-2026-60606	9.1 CRITICAL
CVE-2026-61059	9.1 CRITICAL

CVE-2026-61201	9.0 CRITICAL
CVE-2026-61204	9.0 CRITICAL

CWE's

CWE	Beschrijving
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor

Getroffen producten

Oracle
PeopleSoft
PeopleSoft Enterprise CC Common Application Objects
PeopleSoft Enterprise HCM Talent Acquisition Manager
Oracle Corporation
PeopleSoft Enterprise CRM Common Objects
PeopleSoft Enterprise FIN Expenses
PeopleSoft Enterprise FIN Program Management
PeopleSoft Enterprise SCM Order Management
PeopleSoft Enterprise SCM eProcurement
PeopleSoft In-Memory Project Discovery

Disclaimer