Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0316

Kwetsbaarheden verholpen in Oracle PeopleSoft Enterprise

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 19-08-2026

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 meerdere kwetsbaarheden verholpen in Oracle PeopleSoft Enterprise PeopleTools, inclusief de modules Integration Broker, Data Mover, Configuration Manager, FIN Common Objects, FIN Lease Administration en CC Common Application Objects, specifiek in versies 8.61 tot en met 8.63 en 9.1 tot en met 9.2.

Duiding

De kwetsbaarheden in Oracle PeopleSoft Enterprise PeopleTools en gerelateerde modules stellen een aanvaller in staat om via netwerktoegang, vaak via HTTP of Oracle Net, zonder authenticatie of met lage privileges, het systeem volledig over te nemen of kritieke data te creëren, wijzigen of verwijderen. Sommige kwetsbaarheden vereisen gebruikersinteractie, andere niet. De impact betreft de vertrouwelijkheid, integriteit en beschikbaarheid van het systeem en de data. De kwetsbaarheden omvatten onder meer het omzeilen van authenticatie, privilege-escalatie, en het uitvoeren van ongeautoriseerde acties. Specifieke componenten zoals de Integration Broker en Configuration Manager zijn ook getroffen. De CVSS 3.1 basis scores variëren van 4.4 tot 9.8, waarbij meerdere kwetsbaarheden een hoge score hebben die duidt op een significante impact op de beveiliging van de systemen.

Oplossingen

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

Referenties

- https://www.oracle.com/security-alerts/cspuaug2026.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-60742	8.1 HIGH
CVE-2026-60821	9.8 CRITICAL
CVE-2026-60831	8.1 HIGH
CVE-2026-60856	7.4 HIGH

CVE-2026-60873	7.2 HIGH
CVE-2026-60879	8.8 HIGH
CVE-2026-60883	7.2 HIGH
CVE-2026-60884	4.4 MEDIUM
CVE-2026-60902	7.0 HIGH
CVE-2026-60967	8.8 HIGH
CVE-2026-60975	7.5 HIGH
CVE-2026-61307	8.1 HIGH
CVE-2026-70861	7.2 HIGH
CVE-2026-71092	7.5 HIGH
CVE-2026-71112	8.1 HIGH

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 PeopleTools

Oracle Corporation
PeopleSoft Enterprise FIN Common Objects
PeopleSoft Enterprise FIN Common Objects Brazil
PeopleSoft Enterprise FIN Lease Administration

Disclaimer