Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0340

Kwetsbaarheden verholpen in Oracle PeopleSoft

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 23-10-2025

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 kwetsbaarheden verholpen in Oracle PeopleSoft (Specifiek voor versies 8.60, 8.61, 8.62 en 9.2).

Duiding

De kwetsbaarheden in Oracle PeopleSoft stellen aanvallers in staat om ongeautoriseerde toegang te verkrijgen tot gevoelige gegevens en kunnen leiden tot gegevensmanipulatie. Dit omvat kwetsbaarheden die het mogelijk maken voor zowel laag- als hooggeprivilegieerde aanvallers om via HTTP toegang te krijgen tot kritieke data, met een CVSS-score variërend van 4.3 tot 7.5, wat wijst op aanzienlijke risico's voor de vertrouwelijkheid en integriteit van de gegevens. De kwetsbaarheden zijn te vinden in verschillende componenten zoals OpenSearch Dashboards, PeopleTools, en IT Asset Management.

Oplossingen

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

Referenties

- https://www.oracle.com/security-alerts/cpuoct2025.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-54160	5.1 MEDIUM
CVE-2025-4517	6.9 MEDIUM
CVE-2025-4575	4.8 MEDIUM
CVE-2025-31672	6.9 MEDIUM
CVE-2025-48734	8.1 HIGH
CVE-2025-48924	6.5 MEDIUM
CVE-2025-50181	2.1 LOW
CVE-2025-53048	5.4 MEDIUM

CVE-2025-53050	7.5 HIGH
CVE-2025-53055	6.1 MEDIUM
CVE-2025-53059	4.9 MEDIUM
CVE-2025-53061	5.5 MEDIUM
CVE-2025-53063	5.4 MEDIUM
CVE-2025-53065	5.4 MEDIUM
CVE-2025-61750	4.3 MEDIUM
CVE-2025-61758	6.5 MEDIUM
CVE-2025-61761	5.4 MEDIUM
CVE-2025-61762	6.3 MEDIUM

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-125	Out-of-bounds Read
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-284	Improper Access Control
CWE-295	Improper Certificate Validation
CWE-400	Uncontrolled Resource Consumption
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
CWE-674	Uncontrolled Recursion

Getroffen producten

Oracle
PeopleSoft
PeopleSoft Enterprise CS Financial Aid
PeopleSoft Enterprise FIN IT Asset Management
PeopleSoft Enterprise FIN Maintenance Management
PeopleSoft Enterprise FIN Payables
PeopleSoft Enterprise PeopleTools

Disclaimer