Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0023

Kwetsbaarheden verholpen in Oracle PeopleSoft

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 22-01-2025

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 meerdere kwetsbaarheden verholpen in Oracle PeopleSoft, specifiek in de versies 8.60, 8.61 en 9.2.

Duiding

De kwetsbaarheden in Oracle PeopleSoft stellen geauthenticeerde kwaadwillenden in staat om via HTTP-netwerktoegang ongeautoriseerde toegang te krijgen tot specifieke gegevens, wat kan leiden tot ongeautoriseerde gegevensmanipulatie en -toegang. Kwaadwillenden kunnen ook een Denial-of-Service veroorzaken. Hiervoor heeft de kwaadwillende geen voorafgaande authenticatie nodig.

Oplossingen

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

Referenties

- https://www.oracle.com/security-alerts/cpujan2025.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2020-22218	7.5 HIGH
CVE-2023-48795	7.5 HIGH
CVE-2024-0397	7.5 HIGH
CVE-2024-2511	9.1 CRITICAL
CVE-2024-4030	7.5 HIGH
CVE-2024-4032	7.5 HIGH
CVE-2024-4603	9.1 CRITICAL
CVE-2024-4741	
CVE-2024-5535	9.1 CRITICAL

CVE-2024-6119	9.1 CRITICAL
CVE-2024-6232	7.5 HIGH
CVE-2024-7592	7.5 HIGH
CVE-2024-22018	7.1 HIGH
CVE-2024-22019	8.2 HIGH
CVE-2024-22020	8.2 HIGH
CVE-2024-27280	9.8 CRITICAL
CVE-2024-27281	
CVE-2024-27282	8.1 HIGH
CVE-2024-28849	6.5 MEDIUM
CVE-2024-29025	7.3 HIGH
CVE-2024-35195	5.7 MEDIUM
CVE-2024-36137	7.1 HIGH
CVE-2024-36138	10.0 CRITICAL
CVE-2024-37372	7.1 HIGH
CVE-2024-37891	4.4 MEDIUM
CVE-2024-38998	9.8 CRITICAL
CVE-2024-38999	10.0 CRITICAL
CVE-2025-21530	4.3 MEDIUM
CVE-2025-21537	5.4 MEDIUM
CVE-2025-21539	5.4 MEDIUM
CVE-2025-21545	7.5 HIGH
CVE-2025-21561	5.4 MEDIUM

CVE-2025-21562	**4.3 MEDIUM**
CVE-2025-21563	**4.3 MEDIUM**

CWE's

CWE	Beschrijving
CWE-670	Always-Incorrect Control Flow Implementation
CWE-1395	Dependency on Vulnerable Third-Party Component
CWE-669	Incorrect Resource Transfer Between Spheres
CWE-126	Buffer Over-read
CWE-125	Out-of-bounds Read
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-400	Uncontrolled Resource Consumption
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-787	Out-of-bounds Write
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Getroffen producten

oracle
peoplesoft_enterprise_cc_common_application_objects
peoplesoft_enterprise_fin_cash_management
peoplesoft_enterprise_fin_esettlements
peoplesoft_enterprise_hcm_human_resources
peoplesoft_enterprise_hcm_shared_components
peoplesoft_enterprise_peopletools

peoplesoft_enterprise_scm_purchasing

Disclaimer