Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0170

Kwetsbaarheden verholpen in Oracle E-Business Suite componenten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 29-05-2026

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 kwetsbaarheden verholpen in verschillende componenten van Oracle E-Business Suite, waaronder Oracle Payments, Oracle Internet Procurement Connector, Oracle Financials Common Modules, Oracle iAssets, Oracle Public Sector Financials (International), Oracle Universal Work Queue, Oracle Payroll en Oracle Flow Manufacturing, specifiek in versies 12.2.3 tot en met 12.2.15.

Duiding

De kwetsbaarheden maken het mogelijk voor een aanvaller, vaak met lage privileges en via netwerktoegang over HTTP of HTTPS, om kritieke acties uit te voeren zoals het verkrijgen van volledige systeemcompromittatie, het creëren, verwijderen of wijzigen van belangrijke data, en het uitvoeren van SQL-injecties. Sommige kwetsbaarheden stellen een aanvaller in staat om volledige controle over het systeem te verkrijgen, terwijl andere leiden tot ongeautoriseerde toegang en manipulatie van gevoelige gegevens. De kwetsbaarheden zijn aanwezig in verschillende Oracle-producten binnen de genoemde versies en kunnen leiden tot compromittering van vertrouwelijkheid, integriteit en beschikbaarheid van systemen en data.

Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden in de genoemde componenten van Oracle E-Business Suite te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.oracle.com/security-alerts/cspumay2026.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-46817	9.8 CRITICAL
CVE-2026-46818	7.4 HIGH
CVE-2026-46819	9.1 CRITICAL
CVE-2026-46820	8.5 HIGH
CVE-2026-46821	7.7 HIGH

CVE-2026-46822	9.9 CRITICAL
CVE-2026-46823	7.7 HIGH
CVE-2026-46824	9.9 CRITICAL
CVE-2026-46826	8.8 HIGH
CVE-2026-46827	8.8 HIGH
CVE-2026-46828	8.1 HIGH
CVE-2026-46837	8.8 HIGH

CWE's

CWE	Beschrijving
CWE-190	Integer Overflow or Wraparound
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-125	Out-of-bounds Read
CWE-522	Insufficiently Protected Credentials
CWE-1287	Improper Validation of Specified Type of Input
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')

Getroffen producten

Oracle
E-Business Suite
Oracle Universal Work Queue

Oracle Corporation
Oracle Financials Common Modules
Oracle Flow Manufacturing
Oracle Internet Procurement Connector
Oracle Payments
Oracle Payroll
Oracle Public Sector Financials (International)
Oracle iAssets

Disclaimer