Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0201

Kwetsbaarheden verholpen in Oracle E-Business Suite producten

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 17-06-2026

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 diverse Oracle E-Business Suite producten, waaronder Oracle Enterprise Command Center Framework, iSupplier Portal, Complex Maintenance, Repair and Overhaul, Process Manufacturing Product Development, HR Intelligence, Receivables, Spares Management, Cost Management, Enterprise Asset Management, Applications Manager, iSupport, Advanced Outbound Telephony, Quality, HRMS (UK), Human Resources, Property Manager, Subledger Accounting, Project Portfolio Analysis, Universal Work Queue, Public Sector Financials (International), Financials for EMEA, Outsourced Manufacturing, en Public Sector Payroll.

Duiding

De kwetsbaarheden stellen een aanvaller met netwerktoegang en vaak lage tot hoge privileges in staat om ongeautoriseerde acties uit te voeren, waaronder het verkrijgen van volledige controle over het systeem, het creëren, wijzigen of verwijderen van kritieke data, en het veroorzaken van gedeeltelijke of volledige Denial-of-Service. Sommige kwetsbaarheden vereisen gebruikersinteractie, andere kunnen worden misbruikt zonder authenticatie. De kwetsbaarheden beïnvloeden de vertrouwelijkheid, integriteit en beschikbaarheid van de systemen. De CVSS 3.1 basis scores variëren van 7.1 tot 9.9, waarbij meerdere kwetsbaarheden een score van 8.8 of hoger hebben. De kwetsbaarheden zijn aanwezig in verschillende versies, voornamelijk tussen 12.2.3 en 12.2.15, en in sommige gevallen ook in versies 15 en 16 van het Enterprise Command Center Framework. Exploitatie kan leiden tot volledige systeemcompromittering en kan ook impact hebben op andere Oracle producten die afhankelijk zijn van de kwetsbare componenten.

Oplossingen

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

Referenties

- https://www.oracle.com/security-alerts/cspujun2026.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-46949	9.1 CRITICAL
CVE-2026-46950	8.8 HIGH

CVE-2026-46951	8.8 HIGH
CVE-2026-46952	8.8 HIGH
CVE-2026-46953	7.2 HIGH
CVE-2026-46955	7.7 HIGH
CVE-2026-46956	7.2 HIGH
CVE-2026-46957	7.5 HIGH
CVE-2026-46958	7.5 HIGH
CVE-2026-46959	7.5 HIGH
CVE-2026-46960	7.2 HIGH
CVE-2026-46961	8.8 HIGH
CVE-2026-46962	8.8 HIGH
CVE-2026-46963	9.9 CRITICAL
CVE-2026-46964	9.9 CRITICAL
CVE-2026-46965	8.7 HIGH
CVE-2026-46966	7.7 HIGH
CVE-2026-46967	8.7 HIGH
CVE-2026-46969	7.2 HIGH
CVE-2026-46970	7.2 HIGH
CVE-2026-46971	7.5 HIGH
CVE-2026-46972	8.8 HIGH
CVE-2026-46973	8.8 HIGH
CVE-2026-46976	8.6 HIGH
CVE-2026-46894	8.6 HIGH

CVE-2026-46895	9.9 CRITICAL
CVE-2026-46896	9.1 CRITICAL
CVE-2026-46897	9.9 CRITICAL
CVE-2026-46898	8.1 HIGH
CVE-2026-46899	9.6 CRITICAL
CVE-2026-46900	9.9 CRITICAL
CVE-2026-46901	9.9 CRITICAL
CVE-2026-46902	9.8 CRITICAL
CVE-2026-46915	8.5 HIGH
CVE-2026-46916	8.8 HIGH
CVE-2026-46918	9.9 CRITICAL
CVE-2026-46922	7.2 HIGH
CVE-2026-46927	9.2 CRITICAL
CVE-2026-46928	8.8 HIGH
CVE-2026-46929	8.8 HIGH
CVE-2026-46930	9.1 CRITICAL
CVE-2026-46931	8.8 HIGH
CVE-2026-46932	7.1 HIGH
CVE-2026-46933	9.9 CRITICAL
CVE-2026-46934	7.5 HIGH
CVE-2026-46935	7.5 HIGH
CVE-2026-46937	8.8 HIGH
CVE-2026-46938	7.2 HIGH

CVE-2026-46939	5.3 MEDIUM
CVE-2026-46940	8.8 HIGH
CVE-2026-46942	8.8 HIGH
CVE-2026-46944	9.1 CRITICAL
CVE-2026-46945	9.1 CRITICAL
CVE-2026-46946	9.1 CRITICAL
CVE-2026-46947	8.8 HIGH

CWE's

CWE	Beschrijving
CWE-285	Improper Authorization

Getroffen producten

Oracle
Oracle Advanced Outbound Telephony
Oracle Applications Manager
Oracle Complex Maintenance, Repair and Overhaul
Oracle Configure to Order
Oracle Cost Management
Oracle Enterprise Asset Management

Oracle Enterprise Command Center Framework
Oracle Financials for EMEA
Oracle HR Intelligence
Oracle HRMS (UK)
Oracle Human Resources
Oracle In-Memory Cost Management for Discrete Industries
Oracle Outsourced Mfg for Discrete Industries
Oracle Process Manufacturing Process Planning
Oracle Process Manufacturing Product Development
Oracle Project Portfolio Analysis
Oracle Property Manager
Oracle Public Sector Financials (International)
Oracle Public Sector Payroll
Oracle Quality
Oracle Receivables
Oracle Spares Management

Oracle Subledger Accounting
Oracle Universal Work Queue
Oracle iSetup
Oracle iSupplier Portal
Oracle iSupport

Disclaimer