Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0310

Kwetsbaarheden verholpen in Oracle E-Business Suite

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 kwetsbaarheden verholpen in verschillende componenten van Oracle E-Business Suite, waaronder General Ledger, Payments, Workflow, Sales, Purchasing, Call Center Technology, en andere modules binnen de versies 12.2.3 tot en met 12.2.15.

Duiding

De kwetsbaarheden in Oracle E-Business Suite versies 12.2.3 tot 12.2.15 stellen een aanvaller in staat met lage tot hoge privileges en netwerktoegang via HTTP of HTTPS om ongeautoriseerde acties uit te voeren. Deze acties omvatten het creëren, verwijderen, wijzigen of lezen van kritieke data, het verkrijgen van ongeautoriseerde toegang tot gevoelige informatie, en in sommige gevallen het volledig overnemen van het systeem. Sommige kwetsbaarheden vereisen gebruikersinteractie, terwijl andere zonder authenticatie kunnen worden misbruikt. De impact strekt zich uit over vertrouwelijkheid, integriteit en beschikbaarheid van systemen en data. Daarnaast zijn er kwetsbaarheden die Denial-of-Service kunnen veroorzaken door het laten vastlopen of crashen van applicatiecomponenten. De kwetsbaarheden zijn aanwezig in diverse modules zoals financiële administratie, betalingsverwerking, workflowbeheer, verkoop, inkoop, klantenservice, en andere bedrijfsprocessen binnen de Oracle E-Business Suite.

Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden in Oracle E-Business Suite versies 12.2.3 tot en met 12.2.15 te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

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

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-60693	7.1 HIGH
CVE-2026-60748	7.6 HIGH
CVE-2026-60759	7.4 HIGH
CVE-2026-60769	7.5 HIGH

CVE-2026-60781	7.1 HIGH
CVE-2026-60782	9.8 CRITICAL
CVE-2026-60830	6.5 MEDIUM
CVE-2026-60976	8.8 HIGH
CVE-2026-61139	6.3 MEDIUM
CVE-2026-61198	6.5 MEDIUM
CVE-2026-61296	7.6 HIGH
CVE-2026-61306	7.1 HIGH
CVE-2026-61319	8.8 HIGH
CVE-2026-61331	7.7 HIGH
CVE-2026-61340	8.2 HIGH
CVE-2026-62448	8.2 HIGH
CVE-2026-62449	7.0 HIGH
CVE-2026-62450	8.8 HIGH
CVE-2026-62458	7.1 HIGH
CVE-2026-62462	8.8 HIGH
CVE-2026-62475	6.6 MEDIUM
CVE-2026-62491	8.1 HIGH
CVE-2026-62540	7.2 HIGH
CVE-2026-62599	8.6 HIGH
CVE-2026-62600	8.1 HIGH
CVE-2026-62601	7.1 HIGH
CVE-2026-62605	8.2 HIGH

CVE-2026-62607	8.7 HIGH
CVE-2026-70680	7.1 HIGH
CVE-2026-70681	7.5 HIGH
CVE-2026-70686	8.8 HIGH
CVE-2026-70687	7.7 HIGH
CVE-2026-70690	8.0 HIGH
CVE-2026-70692	7.7 HIGH
CVE-2026-70694	7.7 HIGH
CVE-2026-70695	7.7 HIGH
CVE-2026-70696	7.5 HIGH
CVE-2026-70699	7.4 HIGH
CVE-2026-70700	7.5 HIGH
CVE-2026-70701	8.1 HIGH
CVE-2026-70702	8.2 HIGH
CVE-2026-70704	8.1 HIGH
CVE-2026-70706	7.5 HIGH
CVE-2026-70707	8.8 HIGH
CVE-2026-70708	8.1 HIGH
CVE-2026-70710	8.8 HIGH
CVE-2026-70713	7.5 HIGH
CVE-2026-70718	8.5 HIGH
CVE-2026-70720	6.5 MEDIUM
CVE-2026-70722	8.2 HIGH

CVE-2026-70725	7.6 HIGH
CVE-2026-70726	6.0 MEDIUM
CVE-2026-70729	8.8 HIGH
CVE-2026-70732	6.5 MEDIUM
CVE-2026-70747	8.8 HIGH
CVE-2026-70760	7.1 HIGH
CVE-2026-70761	8.8 HIGH
CVE-2026-70762	8.1 HIGH
CVE-2026-70763	7.5 HIGH
CVE-2026-70764	7.6 HIGH
CVE-2026-70770	8.3 HIGH
CVE-2026-70771	7.7 HIGH
CVE-2026-70772	7.5 HIGH
CVE-2026-70773	8.2 HIGH
CVE-2026-70774	7.1 HIGH
CVE-2026-70775	6.3 MEDIUM
CVE-2026-70777	7.5 HIGH
CVE-2026-70778	8.7 HIGH
CVE-2026-70779	7.4 HIGH
CVE-2026-70781	7.2 HIGH
CVE-2026-70782	8.1 HIGH
CVE-2026-70783	7.4 HIGH
CVE-2026-70786	7.6 HIGH

CVE-2026-70790	7.4 HIGH
CVE-2026-70791	7.6 HIGH
CVE-2026-70792	8.8 HIGH
CVE-2026-70795	8.1 HIGH
CVE-2026-70796	7.2 HIGH
CVE-2026-70797	7.2 HIGH
CVE-2026-70798	7.8 HIGH
CVE-2026-70799	7.5 HIGH
CVE-2026-70800	7.3 HIGH
CVE-2026-70801	7.1 HIGH
CVE-2026-70802	8.0 HIGH
CVE-2026-70803	7.6 HIGH
CVE-2026-70804	7.7 HIGH
CVE-2026-70805	8.1 HIGH
CVE-2026-70806	7.1 HIGH
CVE-2026-70807	8.5 HIGH
CVE-2026-70808	7.1 HIGH
CVE-2026-70809	7.1 HIGH
CVE-2026-70810	7.5 HIGH
CVE-2026-70811	8.1 HIGH
CVE-2026-70812	8.8 HIGH
CVE-2026-70813	8.8 HIGH
CVE-2026-70814	8.1 HIGH

CVE-2026-70815	8.1 HIGH
CVE-2026-70816	7.1 HIGH
CVE-2026-70820	7.2 HIGH
CVE-2026-70827	7.7 HIGH
CVE-2026-70829	7.5 HIGH
CVE-2026-70830	8.1 HIGH
CVE-2026-70833	7.1 HIGH
CVE-2026-70835	8.1 HIGH
CVE-2026-70837	7.1 HIGH
CVE-2026-70839	7.1 HIGH
CVE-2026-70844	7.1 HIGH
CVE-2026-70845	7.1 HIGH
CVE-2026-70918	8.8 HIGH
CVE-2026-70926	9.8 CRITICAL
CVE-2026-70927	7.5 HIGH
CVE-2026-70930	7.5 HIGH
CVE-2026-70931	8.1 HIGH
CVE-2026-70932	7.2 HIGH
CVE-2026-70941	8.8 HIGH
CVE-2026-70945	7.7 HIGH
CVE-2026-70947	7.5 HIGH
CVE-2026-70948	8.8 HIGH
CVE-2026-71101	7.8 HIGH

CVE-2026-71104	7.2 HIGH

CWE's

CWE	Beschrijving
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor

Getroffen producten

Oracle
E-Business Suite
Oracle Customer Care
Oracle MES for Process Manufacturing
Oracle Scripting
Oracle Teleservice
Oracle Workflow
Oracle iSupplier Portal
Oracle Corporation
Oracle Advanced Inbound Telephony
Oracle Applications DBA
Oracle Applications Platform Engineering

Oracle Bills of Material
Oracle Call Center Technology
Oracle Cash Management
Oracle Complex Maintenance, Repair and Overhaul
Oracle Customers Online
Oracle E-Business Tax
Oracle Email Center
Oracle Enterprise Asset Management
Oracle Financials Common Modules
Oracle Flow Manufacturing
Oracle General Ledger
Oracle HCM Common Architecture
Oracle HRMS (Netherlands)
Oracle Installed Base
Oracle Internet Procurement Connector
Oracle Labor Distribution

Oracle Landed Cost Management
Oracle Loans
Oracle Marketing
Oracle Marketing Encyclopedia System
Oracle Mobile Application Server
Oracle Operations Intelligence
Oracle Order Management
Oracle Partner Management
Oracle Payables
Oracle Payments
Oracle Payroll
Oracle Process Manufacturing Systems
Oracle Product Hub
Oracle Production Scheduling
Oracle Project Planning and Control
Oracle Proposals

Oracle Public Sector Financials (International)
Oracle Public Sector Human Resources
Oracle Purchasing
Oracle Risk Management
Oracle SDP Number Portability
Oracle Sales
Oracle Sales Foundation
Oracle Sales for Handhelds
Oracle Service Contracts
Oracle Service Fulfillment Manager
Oracle Shipping Execution
Oracle Telecommunications Billing Integrator
Oracle Trading Community
Oracle Transportation Execution
Oracle Warehouse Management
Oracle Work in Process

Oracle Yard Management
Oracle iRecruitment
Oracle iSetup

Disclaimer