Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0376

Kwetsbaarheden verholpen in Oracle E-Business Suite

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 16-09-2026

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 159 kwetsbaarheden verholpen in diverse Oracle E-Business Suite-producten, waaronder Oracle Applications Framework, Oracle Document Management and Collaboration, Oracle Mobile Application Server, Oracle Alert, Oracle Application Object Library, Oracle Applications Manager, Oracle Bills of Material, Oracle Complex Maintenance, Repair and Overhaul, Oracle Contract Lifecycle Management for Public Sector, Oracle Contracts, Oracle Customer Interaction History, Oracle Demand Signal Repository, Oracle Depot Repair, Oracle Marketing, Oracle Product Hub, Oracle Purchasing, Oracle Report Manager, Oracle Sales Online, Oracle Spares Management, Oracle User Management, Oracle iStore, Oracle HRMS (India), Oracle iRecruitment, Oracle Product Workbench, Oracle Financials for Asia/Pacific, Oracle Engineering, Oracle CRM Technical Foundation, Oracle Financials Common Modules, Oracle Installed Base, Oracle One-to-One Fulfillment, Oracle Order Management, Oracle Project Intelligence, Oracle Work in Process, Oracle Advanced Benefits, Applications DBA, Enterprise Command Center Framework, Oracle Field Service, Oracle Proposals, Oracle Sales, Oracle Sales Offline, Oracle Web Applications Desktop Integrator, Oracle Quality, Oracle Sourcing, Oracle Common Applications, Oracle Lease and Finance Management, Oracle Common Applications Calendar, Oracle Partner Management, Oracle Site Hub, Oracle US Federal Human Resources, Oracle XML Gateway, Oracle HR Intelligence, Oracle Assets en Oracle Process Manufacturing Intelligence.

Duiding

De kwetsbaarheden betreffen verschillende beveiligingsproblemen in Oracle E-Business Suite-producten, waaronder mogelijkheden voor niet-geauthenticeerde en laaggeprivilegieerde kwaadwillenden om via netwerktoegang ongeautoriseerde acties uit te voeren. De kwetsbaarheden hebben CVSS-scores variërend van middel tot kritiek. Van de in totaal 159 kwetsbaarheden zijn drie als kritiek aangemerkt en volgens Oracle kunnen 19 kwetsbaarheden zonder authenticatie op afstand worden misbruikt. Succesvol misbruik kan onder meer leiden tot het verkrijgen van ongeautoriseerde toegang tot gevoelige informatie, het wijzigen of verwijderen van gegevens, volledige overname van getroffen componenten en het verstoren van de beschikbaarheid van getroffen systemen. Sommige kwetsbaarheden vereisen gebruikersinteractie of voorafgaande toegangsrechten, terwijl andere volledig op afstand en zonder authenticatie kunnen worden misbruikt.

De drie kwetsbaarheden die als kritiek zijn aangemerkt, CVE-2026-83327, CVE-2026-83452 en CVE-2026-83462, hebben een CVSS-score van 9,8 en bevinden zich respectievelijk in Oracle Applications Framework, Oracle Document Management and Collaboration en Oracle Mobile Application Server. Deze kwetsbaarheden kunnen zonder authenticatie op afstand worden misbruikt, vereisen een lage aanvalscomplexiteit en geen gebruikersinteractie. Succesvolle exploitatie kan leiden tot volledige overname van de getroffen component en heeft een hoge impact op de vertrouwelijkheid, integriteit en beschikbaarheid van getroffen systemen.

Het NCSC adviseert om de beveiligingsupdates voor de kritieke kwetsbaarheden met voorrang toe te passen.

Oplossingen

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

Referenties

- https://www.oracle.com/security-alerts/cspusep2026.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-70755	6.5 MEDIUM
CVE-2026-83044	7.1 HIGH
CVE-2026-83072	8.1 HIGH
CVE-2026-83076	6.8 MEDIUM
CVE-2026-83082	7.2 HIGH
CVE-2026-83083	8.5 HIGH
CVE-2026-83084	7.7 HIGH
CVE-2026-83089	8.1 HIGH
CVE-2026-83090	8.8 HIGH
CVE-2026-83091	7.6 HIGH
CVE-2026-83092	7.1 HIGH
CVE-2026-83110	7.5 HIGH
CVE-2026-83111	7.1 HIGH
CVE-2026-83112	7.2 HIGH
CVE-2026-83113	7.1 HIGH

CVE-2026-83114	7.5 HIGH
CVE-2026-83115	7.5 HIGH
CVE-2026-83116	7.7 HIGH
CVE-2026-83117	7.2 HIGH
CVE-2026-83118	7.8 HIGH
CVE-2026-83119	8.8 HIGH
CVE-2026-83120	8.8 HIGH
CVE-2026-83121	8.8 HIGH
CVE-2026-83122	8.8 HIGH
CVE-2026-83123	7.1 HIGH
CVE-2026-83124	8.8 HIGH
CVE-2026-83125	8.8 HIGH
CVE-2026-83126	7.6 HIGH
CVE-2026-83127	7.7 HIGH
CVE-2026-83128	7.5 HIGH
CVE-2026-83129	7.7 HIGH
CVE-2026-83130	7.1 HIGH
CVE-2026-83131	7.7 HIGH
CVE-2026-83132	8.1 HIGH
CVE-2026-83133	7.5 HIGH
CVE-2026-83134	7.7 HIGH
CVE-2026-83135	8.7 HIGH
CVE-2026-83136	8.8 HIGH

CVE-2026-83137	8.8 HIGH
CVE-2026-83138	8.0 HIGH
CVE-2026-83140	6.5 MEDIUM
CVE-2026-83141	7.7 HIGH
CVE-2026-83142	7.7 HIGH
CVE-2026-83152	8.1 HIGH
CVE-2026-83157	8.0 HIGH
CVE-2026-83158	7.1 HIGH
CVE-2026-83159	7.8 HIGH
CVE-2026-83161	7.1 HIGH
CVE-2026-83162	7.4 HIGH
CVE-2026-83163	8.8 HIGH
CVE-2026-83164	8.8 HIGH
CVE-2026-83165	8.8 HIGH
CVE-2026-83166	7.7 HIGH
CVE-2026-83167	7.5 HIGH
CVE-2026-83168	8.8 HIGH
CVE-2026-83169	8.1 HIGH
CVE-2026-83170	8.0 HIGH
CVE-2026-83171	7.1 HIGH
CVE-2026-83172	8.5 HIGH
CVE-2026-83173	7.1 HIGH
CVE-2026-83174	8.1 HIGH

CVE-2026-83175	6.5 MEDIUM
CVE-2026-83176	7.2 HIGH
CVE-2026-83177	8.1 HIGH
CVE-2026-83178	8.0 HIGH
CVE-2026-83179	7.1 HIGH
CVE-2026-83184	7.4 HIGH
CVE-2026-83185	7.3 HIGH
CVE-2026-83186	7.1 HIGH
CVE-2026-83187	7.1 HIGH
CVE-2026-83188	7.2 HIGH
CVE-2026-83189	8.8 HIGH
CVE-2026-83194	8.8 HIGH
CVE-2026-83198	5.4 MEDIUM
CVE-2026-83200	6.5 MEDIUM
CVE-2026-83204	7.5 HIGH
CVE-2026-83205	8.8 HIGH
CVE-2026-83300	7.1 HIGH
CVE-2026-83327	9.8 CRITICAL
CVE-2026-83328	7.2 HIGH
CVE-2026-83329	8.8 HIGH
CVE-2026-83331	8.8 HIGH
CVE-2026-83332	7.1 HIGH
CVE-2026-83338	8.8 HIGH

CVE-2026-83341	7.5 HIGH
CVE-2026-83345	7.1 HIGH
CVE-2026-83352	7.1 HIGH
CVE-2026-83356	7.7 HIGH
CVE-2026-83425	8.5 HIGH
CVE-2026-83428	8.1 HIGH
CVE-2026-83429	8.1 HIGH
CVE-2026-83430	8.1 HIGH
CVE-2026-83431	5.4 MEDIUM
CVE-2026-83432	8.1 HIGH
CVE-2026-83433	6.5 MEDIUM
CVE-2026-83434	8.1 HIGH
CVE-2026-83435	8.2 HIGH
CVE-2026-83436	7.1 HIGH
CVE-2026-83437	7.7 HIGH
CVE-2026-83438	8.2 HIGH
CVE-2026-83440	7.2 HIGH
CVE-2026-83441	6.8 MEDIUM
CVE-2026-83442	7.2 HIGH
CVE-2026-83443	6.5 MEDIUM
CVE-2026-83444	8.8 HIGH
CVE-2026-83445	8.8 HIGH
CVE-2026-83446	8.1 HIGH

CVE-2026-83447	8.1 HIGH
CVE-2026-83448	8.1 HIGH
CVE-2026-83449	8.5 HIGH
CVE-2026-83450	8.0 HIGH
CVE-2026-83451	8.5 HIGH
CVE-2026-83452	9.8 CRITICAL
CVE-2026-83453	7.2 HIGH
CVE-2026-83454	8.8 HIGH
CVE-2026-83455	8.1 HIGH
CVE-2026-83456	8.8 HIGH
CVE-2026-83457	8.1 HIGH
CVE-2026-83461	8.2 HIGH
CVE-2026-83462	9.8 CRITICAL
CVE-2026-83463	7.5 HIGH
CVE-2026-83464	8.1 HIGH
CVE-2026-83465	8.2 HIGH
CVE-2026-83477	8.1 HIGH
CVE-2026-83479	8.8 HIGH
CVE-2026-83481	7.2 HIGH
CVE-2026-83482	7.2 HIGH
CVE-2026-83483	8.0 HIGH
CVE-2026-83484	7.1 HIGH
CVE-2026-83485	7.7 HIGH

CVE-2026-83486	7.7 HIGH
CVE-2026-83487	7.7 HIGH
CVE-2026-83490	8.5 HIGH
CVE-2026-83491	6.8 MEDIUM
CVE-2026-87124	7.7 HIGH
CVE-2026-87125	8.3 HIGH
CVE-2026-87126	7.1 HIGH
CVE-2026-87127	7.7 HIGH
CVE-2026-87149	7.1 HIGH
CVE-2026-87150	8.8 HIGH
CVE-2026-87151	7.7 HIGH
CVE-2026-87152	8.1 HIGH
CVE-2026-87153	8.1 HIGH
CVE-2026-87154	8.1 HIGH
CVE-2026-87155	8.8 HIGH
CVE-2026-87156	7.1 HIGH
CVE-2026-87157	8.1 HIGH
CVE-2026-87158	7.1 HIGH
CVE-2026-87159	8.1 HIGH
CVE-2026-87160	7.1 HIGH
CVE-2026-87161	8.5 HIGH
CVE-2026-87162	8.8 HIGH
CVE-2026-87163	8.8 HIGH

CVE-2026-87165	8.8 HIGH
CVE-2026-87166	8.1 HIGH
CVE-2026-87167	8.1 HIGH
CVE-2026-87168	8.1 HIGH
CVE-2026-87169	6.1 MEDIUM
CVE-2026-87265	8.1 HIGH

CWE's

CWE	Beschrijving
CWE-306	Missing Authentication for Critical Function

Getroffen producten

Oracle
Oracle Application Object Library
Oracle Applications Framework
Oracle Applications Manager
Oracle Document Management and Collaboration
Oracle Mobile Application Server

Disclaimer