Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0306

Kwetsbaarheden verholpen in Oracle Fusion Middleware

NCSC Security Advisory

PRIORITEIT: HOOG

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 262 kwetsbaarheden verholpen in diverse Oracle producten, waaronder Oracle WebLogic Server, Oracle Identity Manager, Oracle WebCenter Portal, Oracle WebCenter Content, Oracle WebCenter Sites, Oracle WebCenter Enterprise Capture, Oracle Reports Developer, Oracle Fusion Middleware Helidon, Oracle Access Manager, Oracle Unified Directory, Oracle Virtual Directory, Oracle Internet Directory, Oracle Web Services Manager, Oracle SOA Suite B2B Engine, Oracle Managed File Transfer, en Oracle Identity Manager Connector.

Duiding

De kwetsbaarheden betreffen verschillende beveiligingsproblemen in Oracle producten, waaronder mogelijkheden voor ongeauthenticeerde en laaggeprivilegieerde aanvallers om via netwerktoegang (HTTP, HTTPS, HTTP/2, LDAP, T3, IIOP, RMI, CORBA, SOAP, SMTP, UDP) ongeautoriseerde acties uit te voeren. Deze acties omvatten het verkrijgen van volledige systeemcontrole, het uitvoeren van arbitrary code, het creëren, wijzigen of verwijderen van kritieke data, het omzeilen van authenticatiecontroles, het verkrijgen van ongeautoriseerde toegang tot gevoelige informatie, en het veroorzaken van Denial-of-Service (DoS) door crashes of resource-uitputting. Sommige kwetsbaarheden vereisen gebruikersinteractie, terwijl andere volledig op afstand en zonder authenticatie kunnen worden misbruikt.

De CVSS 3.1 basis scores variëren van matig tot maximaal (tot 10.0), waarbij meerdere kwetsbaarheden een score van 9.8 of hoger hebben, wat duidt op een hoog potentieel voor impact op vertrouwelijkheid, integriteit en beschikbaarheid van de systemen. 182 van deze kwetsbaarheden kunnen zonder voorafgaande authenticatie op afstand worden misbruikt. De kwetsbaarheden zijn specifiek voor bepaalde versies van de genoemde Oracle producten maar kunnen ook invloed hebben op andere Oracle producten die afhankelijk zijn van deze componenten.

Het NCSC adviseert om deze kwetsbaarheden met voorrang te verhelpen.

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/cspuaug2026.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-33186	9.1 CRITICAL
CVE-2026-42587	7.5 HIGH
CVE-2026-60392	7.8 HIGH
CVE-2026-60412	7.8 HIGH
CVE-2026-60413	7.8 HIGH
CVE-2026-60414	7.8 HIGH
CVE-2026-60415	8.1 HIGH
CVE-2026-60672	9.8 CRITICAL
CVE-2026-60679	7.5 HIGH
CVE-2026-60680	8.1 HIGH
CVE-2026-60696	9.8 CRITICAL
CVE-2026-60698	9.8 CRITICAL
CVE-2026-60699	8.6 HIGH
CVE-2026-60702	9.9 CRITICAL
CVE-2026-60707	8.7 HIGH
CVE-2026-60715	8.8 HIGH
CVE-2026-60716	8.8 HIGH
CVE-2026-60720	9.9 CRITICAL
CVE-2026-60721	9.8 CRITICAL
CVE-2026-60722	8.8 HIGH
CVE-2026-60726	8.8 HIGH

CVE-2026-60727	9.8 CRITICAL
CVE-2026-60728	9.1 CRITICAL
CVE-2026-60729	8.8 HIGH
CVE-2026-60730	9.9 CRITICAL
CVE-2026-60731	8.8 HIGH
CVE-2026-60733	7.7 HIGH
CVE-2026-60737	9.1 CRITICAL
CVE-2026-60841	8.5 HIGH
CVE-2026-60849	8.5 HIGH
CVE-2026-60850	7.5 HIGH
CVE-2026-60853	3.7 LOW
CVE-2026-60860	8.7 HIGH
CVE-2026-60861	9.6 CRITICAL
CVE-2026-60865	6.8 MEDIUM
CVE-2026-60866	6.5 MEDIUM
CVE-2026-60889	7.5 HIGH
CVE-2026-60895	6.8 MEDIUM
CVE-2026-60903	8.7 HIGH
CVE-2026-60905	9.6 CRITICAL
CVE-2026-60906	7.5 HIGH
CVE-2026-60909	7.6 HIGH
CVE-2026-60914	7.5 HIGH
CVE-2026-60915	7.4 HIGH

CVE-2026-60916	9.9 CRITICAL
CVE-2026-60921	9.8 CRITICAL
CVE-2026-60928	8.4 HIGH
CVE-2026-60933	7.4 HIGH
CVE-2026-60934	8.7 HIGH
CVE-2026-60935	8.7 HIGH
CVE-2026-60944	8.2 HIGH
CVE-2026-60946	9.8 CRITICAL
CVE-2026-60947	9.8 CRITICAL
CVE-2026-60949	7.1 HIGH
CVE-2026-60954	8.7 HIGH
CVE-2026-60955	8.2 HIGH
CVE-2026-60958	9.8 CRITICAL
CVE-2026-60961	8.0 HIGH
CVE-2026-60969	7.7 HIGH
CVE-2026-60970	9.8 CRITICAL
CVE-2026-60971	9.8 CRITICAL
CVE-2026-60977	9.8 CRITICAL
CVE-2026-60980	8.7 HIGH
CVE-2026-60981	8.7 HIGH
CVE-2026-60983	7.7 HIGH
CVE-2026-60990	9.9 CRITICAL
CVE-2026-60991	7.8 HIGH

CVE-2026-60992	8.1 HIGH
CVE-2026-60993	7.5 HIGH
CVE-2026-60994	7.2 HIGH
CVE-2026-60995	9.9 CRITICAL
CVE-2026-60996	8.7 HIGH
CVE-2026-60998	8.0 HIGH
CVE-2026-61001	9.6 CRITICAL
CVE-2026-61002	8.8 HIGH
CVE-2026-61003	9.9 CRITICAL
CVE-2026-61007	7.5 HIGH
CVE-2026-61008	9.1 CRITICAL
CVE-2026-61011	8.2 HIGH
CVE-2026-61016	8.2 HIGH
CVE-2026-61017	8.8 HIGH
CVE-2026-61018	9.8 CRITICAL
CVE-2026-61021	9.9 CRITICAL
CVE-2026-61022	8.8 HIGH
CVE-2026-61029	9.0 CRITICAL
CVE-2026-61032	8.8 HIGH
CVE-2026-61033	8.6 HIGH
CVE-2026-61034	9.1 CRITICAL
CVE-2026-61038	8.2 HIGH
CVE-2026-61040	8.8 HIGH

CVE-2026-61042	8.8 HIGH
CVE-2026-61045	8.6 HIGH
CVE-2026-61054	8.2 HIGH
CVE-2026-61058	8.8 HIGH
CVE-2026-61066	9.9 CRITICAL
CVE-2026-61118	8.8 HIGH
CVE-2026-61124	7.1 HIGH
CVE-2026-61177	8.1 HIGH
CVE-2026-61193	8.7 HIGH
CVE-2026-61199	7.7 HIGH
CVE-2026-61208	7.6 HIGH
CVE-2026-61212	8.5 HIGH
CVE-2026-61213	8.8 HIGH
CVE-2026-61215	8.7 HIGH
CVE-2026-61219	8.7 HIGH
CVE-2026-61222	8.2 HIGH
CVE-2026-61227	7.6 HIGH
CVE-2026-61228	8.6 HIGH
CVE-2026-61229	8.1 HIGH
CVE-2026-61230	8.6 HIGH
CVE-2026-61231	8.8 HIGH
CVE-2026-61241	10.0 CRITICAL
CVE-2026-61248	9.9 CRITICAL

CVE-2026-61258	9.8 CRITICAL
CVE-2026-61288	7.1 HIGH
CVE-2026-61290	7.1 HIGH
CVE-2026-61291	7.8 HIGH
CVE-2026-61295	7.1 HIGH
CVE-2026-62608	9.9 CRITICAL
CVE-2026-62609	9.8 CRITICAL
CVE-2026-62610	9.1 CRITICAL
CVE-2026-62611	9.8 CRITICAL
CVE-2026-62612	8.8 HIGH
CVE-2026-62613	9.3 CRITICAL
CVE-2026-62614	9.8 CRITICAL
CVE-2026-62615	8.5 HIGH
CVE-2026-62616	7.2 HIGH
CVE-2026-62617	9.8 CRITICAL
CVE-2026-62618	9.3 CRITICAL
CVE-2026-62619	8.8 HIGH
CVE-2026-62620	8.6 HIGH
CVE-2026-62621	9.8 CRITICAL
CVE-2026-62622	9.8 CRITICAL
CVE-2026-62623	8.8 HIGH
CVE-2026-62624	9.8 CRITICAL
CVE-2026-62625	8.6 HIGH

CVE-2026-62626	9.8 CRITICAL
CVE-2026-62627	7.1 HIGH
CVE-2026-62628	8.6 HIGH
CVE-2026-62629	9.4 CRITICAL
CVE-2026-62630	9.8 CRITICAL
CVE-2026-62631	8.8 HIGH
CVE-2026-62632	9.8 CRITICAL
CVE-2026-62633	9.8 CRITICAL
CVE-2026-62634	9.8 CRITICAL
CVE-2026-62635	9.8 CRITICAL
CVE-2026-62636	8.6 HIGH
CVE-2026-62637	9.3 CRITICAL
CVE-2026-62638	9.1 CRITICAL
CVE-2026-62639	9.8 CRITICAL
CVE-2026-62640	9.8 CRITICAL
CVE-2026-70668	9.1 CRITICAL
CVE-2026-70669	9.8 CRITICAL
CVE-2026-70670	9.6 CRITICAL
CVE-2026-70671	8.1 HIGH
CVE-2026-70672	7.4 HIGH
CVE-2026-70673	9.3 CRITICAL
CVE-2026-70674	8.8 HIGH
CVE-2026-70675	8.1 HIGH

CVE-2026-70716	5.9 MEDIUM
CVE-2026-70727	5.3 MEDIUM
CVE-2026-70858	7.1 HIGH
CVE-2026-70905	9.8 CRITICAL
CVE-2026-70908	7.5 HIGH
CVE-2026-70923	6.1 MEDIUM
CVE-2026-70924	8.1 HIGH
CVE-2026-70970	9.8 CRITICAL
CVE-2026-71029	6.8 MEDIUM
CVE-2026-71065	9.3 CRITICAL
CVE-2026-71074	9.8 CRITICAL
CVE-2026-71110	8.1 HIGH
CVE-2026-71111	7.8 HIGH
CVE-2026-71124	4.3 MEDIUM
CVE-2026-71152	9.8 CRITICAL
CVE-2026-71153	7.5 HIGH
CVE-2026-71154	6.1 MEDIUM
CVE-2026-71155	8.5 HIGH
CVE-2026-71156	5.3 MEDIUM
CVE-2026-71157	5.3 MEDIUM
CVE-2026-71158	7.5 HIGH
CVE-2026-71159	8.2 HIGH
CVE-2026-71160	7.5 HIGH

CVE-2026-71161	5.3 MEDIUM
CVE-2026-71162	6.5 MEDIUM
CVE-2026-71164	9.8 CRITICAL
CVE-2026-71165	5.4 MEDIUM
CVE-2026-71166	9.4 CRITICAL
CVE-2026-71167	9.4 CRITICAL
CVE-2026-73865	9.1 CRITICAL
CVE-2026-73866	9.1 CRITICAL
CVE-2026-73867	6.5 MEDIUM
CVE-2026-73868	6.5 MEDIUM
CVE-2026-73869	6.1 MEDIUM
CVE-2026-73870	6.1 MEDIUM
CVE-2026-73871	5.3 MEDIUM
CVE-2026-73872	5.3 MEDIUM
CVE-2026-73873	4.2 MEDIUM
CVE-2026-73874	5.4 MEDIUM
CVE-2026-73875	7.2 HIGH
CVE-2026-73876	7.2 HIGH
CVE-2026-73877	5.3 MEDIUM
CVE-2026-73878	7.5 HIGH
CVE-2026-73879	7.5 HIGH
CVE-2026-73880	4.4 MEDIUM
CVE-2026-73881	5.4 MEDIUM

CVE-2026-73882	7.5 HIGH
CVE-2026-73883	7.5 HIGH
CVE-2026-73884	7.5 HIGH
CVE-2026-73885	7.2 HIGH
CVE-2026-73886	7.2 HIGH
CVE-2026-73887	7.5 HIGH
CVE-2026-73888	5.3 MEDIUM
CVE-2026-73889	5.3 MEDIUM
CVE-2026-73890	7.5 HIGH
CVE-2026-73891	7.3 HIGH
CVE-2026-73892	6.5 MEDIUM
CVE-2026-73893	6.5 MEDIUM
CVE-2026-73894	7.3 HIGH
CVE-2026-73895	5.3 MEDIUM
CVE-2026-73896	6.5 MEDIUM
CVE-2026-73897	6.5 MEDIUM
CVE-2026-73898	6.1 MEDIUM
CVE-2026-73899	5.3 MEDIUM
CVE-2026-73900	5.3 MEDIUM
CVE-2026-73901	4.8 MEDIUM
CVE-2026-73902	7.5 HIGH
CVE-2026-73903	7.5 HIGH
CVE-2026-73904	6.5 MEDIUM

CVE-2026-73905	9.8 CRITICAL
CVE-2026-73906	5.3 MEDIUM
CVE-2026-73907	7.5 HIGH
CVE-2026-73908	7.5 HIGH
CVE-2026-73909	5.9 MEDIUM
CVE-2026-73910	5.3 MEDIUM
CVE-2026-73911	5.4 MEDIUM
CVE-2026-73912	9.8 CRITICAL
CVE-2026-73913	5.4 MEDIUM
CVE-2026-73914	6.5 MEDIUM
CVE-2026-73915	7.5 HIGH
CVE-2026-73916	9.1 CRITICAL
CVE-2026-73917	9.1 CRITICAL
CVE-2026-73918	7.3 HIGH
CVE-2026-73919	5.4 MEDIUM
CVE-2026-73920	9.4 CRITICAL
CVE-2026-73921	9.8 CRITICAL
CVE-2026-73922	9.1 CRITICAL
CVE-2026-73923	3.7 LOW
CVE-2026-73924	9.1 CRITICAL
CVE-2026-73925	8.2 HIGH
CVE-2026-73927	7.5 HIGH
CVE-2026-73928	7.2 HIGH

CVE-2026-73929	8.3 HIGH
CVE-2026-73930	9.9 CRITICAL
CVE-2026-73931	8.3 HIGH
CVE-2026-73932	5.3 MEDIUM
CVE-2026-73933	7.3 HIGH
CVE-2026-73934	7.5 HIGH
CVE-2026-73935	7.5 HIGH
CVE-2026-73936	7.5 HIGH
CVE-2026-73937	8.2 HIGH
CVE-2026-73938	7.5 HIGH
CVE-2026-73939	8.6 HIGH

CWE's

CWE	Beschrijving
CWE-285	Improper Authorization
CWE-400	Uncontrolled Resource Consumption
CWE-551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization
CWE-770	Allocation of Resources Without Limits or Throttling

Getroffen producten

Oracle
Fusion Middleware
Oracle WebLogic Server

Oracle Corporation
Helidon
Oracle Access Manager
Oracle Identity Manager
Oracle Identity Manager Connector
Oracle Internet Directory
Oracle Managed File Transfer
Oracle Outside In Technology
Oracle Reports Developer
Oracle SOA Suite
Oracle Unified Directory
Oracle Virtual Directory
Oracle Web Services Manager
Oracle WebCenter Content
Oracle WebCenter Enterprise Capture
Oracle WebCenter Portal
Oracle WebCenter Sites

Service Delivery
Platform

Disclaimer