Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0372

Kwetsbaarheden verholpen in Oracle Fusion Middleware

NCSC Security Advisory

PRIORITEIT: HOOG

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 153 kwetsbaarheden verholpen in diverse Oracle Fusion Middleware-producten, waaronder Helidon, Oracle Access Manager, Oracle Coherence, Oracle Data Integrator, Oracle Forms, Oracle Fusion Middleware Control, Oracle Identity Manager, Oracle Identity Manager Connector, Oracle Internet Directory, Oracle JDeveloper, Oracle Managed File Transfer, Oracle Middleware Common Libraries and Tools, Oracle Platform Security for Java, Oracle Web Services Manager, Oracle WebCenter Content, Oracle WebCenter Enterprise Capture, Oracle WebCenter Portal, Oracle WebCenter Sites, Oracle WebLogic Server en Service Delivery Platform.

Duiding

De kwetsbaarheden betreffen verschillende beveiligingsproblemen in Oracle-producten, waaronder mogelijkheden voor niet-geauthenticeerde en laaggeprivilegieerde kwaadwillenden om via netwerktoegang ongeautoriseerde acties uit te voeren. De kwetsbaarheden hebben CVSS-scores variërend van laag tot kritiek. Van de in totaal 153 kwetsbaarheden zijn 66 als kritiek aangemerkt en volgens Oracle kunnen 78 kwetsbaarheden zonder authenticatie op afstand worden misbruikt. Succesvol misbruik kan onder meer leiden tot het uitvoeren van willekeurige code, het omzeilen van authenticatie- en autorisatiecontroles, het verkrijgen van ongeautoriseerde toegang tot gevoelige informatie, het wijzigen of verwijderen van gegevens en het veroorzaken van Denial-of-Service (DoS). Sommige kwetsbaarheden vereisen gebruikersinteractie of voorafgaande toegangsrechten, terwijl andere volledig op afstand en zonder authenticatie kunnen worden misbruikt.

Van de 66 kwetsbaarheden die als kritiek zijn aangemerkt, hebben meerdere een CVSS-score van 9,8 of hoger. Vijf kwetsbaarheden, CVE-2026-71133, CVE-2026-83099, CVE-2026-83059, CVE-2026-83020 en CVE-2026-83021, hebben een CVSS-score van 10,0 en bevinden zich in Oracle Access Manager, Oracle Forms, Oracle Internet Directory, Oracle Platform Security for Java en Oracle WebLogic Server. Deze kwetsbaarheden kunnen volgens Oracle zonder authenticatie op afstand worden misbruikt en kunnen een hoge impact hebben 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 in de genoemde producten te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

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

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-83025	8.7 HIGH
CVE-2026-83026	8.3 HIGH
CVE-2026-83027	9.3 CRITICAL
CVE-2026-83028	7.5 HIGH
CVE-2026-83029	9.6 CRITICAL
CVE-2026-83030	8.3 HIGH
CVE-2026-83031	9.9 CRITICAL
CVE-2026-83032	8.8 HIGH
CVE-2026-83033	8.8 HIGH
CVE-2026-83034	7.5 HIGH
CVE-2026-83035	9.8 CRITICAL
CVE-2026-83036	9.8 CRITICAL
CVE-2026-83037	9.8 CRITICAL
CVE-2026-83038	9.9 CRITICAL
CVE-2026-83276	7.5 HIGH
CVE-2026-83278	6.8 MEDIUM
CVE-2026-83280	7.5 HIGH
CVE-2026-83281	7.5 HIGH
CVE-2026-83306	8.8 HIGH
CVE-2026-83330	7.5 HIGH
CVE-2026-83334	7.4 HIGH

CVE-2026-83337	7.8 HIGH
CVE-2026-83339	9.8 CRITICAL
CVE-2026-83340	8.8 HIGH
CVE-2026-83344	7.2 HIGH
CVE-2026-83346	5.4 MEDIUM
CVE-2026-83353	7.8 HIGH
CVE-2026-83354	6.3 MEDIUM
CVE-2026-83369	3.1 LOW
CVE-2026-83410	8.8 HIGH
CVE-2026-83411	8.8 HIGH
CVE-2026-83412	8.1 HIGH
CVE-2026-83413	1.9 LOW
CVE-2026-83414	2.5 LOW
CVE-2026-83415	7.5 HIGH
CVE-2026-83416	4.3 MEDIUM
CVE-2026-83422	8.1 HIGH
CVE-2026-83423	8.8 HIGH
CVE-2026-83424	7.5 HIGH
CVE-2026-83439	8.1 HIGH
CVE-2026-83458	5.3 MEDIUM
CVE-2026-83459	5.3 MEDIUM
CVE-2026-83460	6.5 MEDIUM
CVE-2026-83480	5.3 MEDIUM

CVE-2026-83488	5.4 MEDIUM
CVE-2026-87289	7.5 HIGH
CVE-2026-83039	9.9 CRITICAL
CVE-2026-83040	9.6 CRITICAL
CVE-2026-83041	7.7 HIGH
CVE-2026-83042	9.8 CRITICAL
CVE-2026-83043	9.6 CRITICAL
CVE-2026-83045	8.5 HIGH
CVE-2026-83046	7.1 HIGH
CVE-2026-83047	8.2 HIGH
CVE-2026-83048	7.7 HIGH
CVE-2026-83049	8.5 HIGH
CVE-2026-83050	7.1 HIGH
CVE-2026-83051	7.5 HIGH
CVE-2026-83052	7.6 HIGH
CVE-2026-83053	8.8 HIGH
CVE-2026-83054	9.8 CRITICAL
CVE-2026-83055	9.9 CRITICAL
CVE-2026-83056	9.9 CRITICAL
CVE-2026-83057	9.9 CRITICAL
CVE-2026-83058	9.9 CRITICAL
CVE-2026-83059	10.0 CRITICAL
CVE-2026-83060	9.8 CRITICAL

CVE-2026-83061	9.8 CRITICAL
CVE-2026-83062	9.8 CRITICAL
CVE-2026-83063	7.2 HIGH
CVE-2026-83064	9.1 CRITICAL
CVE-2026-83065	7.5 HIGH
CVE-2026-83066	9.8 CRITICAL
CVE-2026-83067	8.1 HIGH
CVE-2026-83069	8.8 HIGH
CVE-2026-83093	8.6 HIGH
CVE-2026-83094	9.8 CRITICAL
CVE-2026-83095	9.8 CRITICAL
CVE-2026-83096	7.9 HIGH
CVE-2026-83097	6.5 MEDIUM
CVE-2026-83098	9.8 CRITICAL
CVE-2026-83099	10.0 CRITICAL
CVE-2026-83100	9.8 CRITICAL
CVE-2026-83101	8.1 HIGH
CVE-2026-83102	7.4 HIGH
CVE-2026-83103	9.1 CRITICAL
CVE-2026-83104	9.1 CRITICAL
CVE-2026-83105	9.0 CRITICAL
CVE-2026-83106	7.5 HIGH
CVE-2026-83107	9.1 CRITICAL

CVE-2026-83108	9.8 CRITICAL
CVE-2026-83109	5.3 MEDIUM
CVE-2026-83151	9.8 CRITICAL
CVE-2026-83231	7.0 HIGH
CVE-2026-83232	9.8 CRITICAL
CVE-2026-83265	8.2 HIGH
CVE-2026-83266	8.2 HIGH
CVE-2026-47065	9.8 CRITICAL
CVE-2026-70748	9.8 CRITICAL
CVE-2026-70756	9.8 CRITICAL
CVE-2026-70757	9.8 CRITICAL
CVE-2026-70913	9.8 CRITICAL
CVE-2026-70915	8.8 HIGH
CVE-2026-71047	8.8 HIGH
CVE-2026-71133	10.0 CRITICAL
CVE-2026-71163	9.9 CRITICAL
CVE-2026-73926	8.7 HIGH
CVE-2026-73940	9.8 CRITICAL
CVE-2026-73941	8.6 HIGH
CVE-2026-73942	8.8 HIGH
CVE-2026-73943	7.6 HIGH
CVE-2026-73944	9.1 CRITICAL
CVE-2026-73945	9.9 CRITICAL

CVE-2026-73946	9.1 CRITICAL
CVE-2026-73947	9.8 CRITICAL
CVE-2026-73948	9.9 CRITICAL
CVE-2026-73949	8.8 HIGH
CVE-2026-73950	9.8 CRITICAL
CVE-2026-73951	8.1 HIGH
CVE-2026-73952	9.1 CRITICAL
CVE-2026-73953	9.8 CRITICAL
CVE-2026-73956	9.8 CRITICAL
CVE-2026-73957	9.3 CRITICAL
CVE-2026-73958	8.1 HIGH
CVE-2026-73959	8.8 HIGH
CVE-2026-73961	9.8 CRITICAL
CVE-2026-73962	9.6 CRITICAL
CVE-2026-73963	9.8 CRITICAL
CVE-2026-82994	9.8 CRITICAL
CVE-2026-82995	9.8 CRITICAL
CVE-2026-82996	7.8 HIGH
CVE-2026-82997	9.9 CRITICAL
CVE-2026-82998	9.9 CRITICAL
CVE-2026-82999	9.9 CRITICAL
CVE-2026-83000	9.8 CRITICAL
CVE-2026-83001	9.1 CRITICAL

CVE-2026-83002	8.5 HIGH
CVE-2026-83003	8.5 HIGH
CVE-2026-83004	7.2 HIGH
CVE-2026-83005	8.8 HIGH
CVE-2026-83006	9.1 CRITICAL
CVE-2026-83007	8.5 HIGH
CVE-2026-83008	8.8 HIGH
CVE-2026-83009	8.8 HIGH
CVE-2026-83010	8.1 HIGH
CVE-2026-83011	8.1 HIGH
CVE-2026-83012	7.7 HIGH
CVE-2026-83013	8.8 HIGH
CVE-2026-83020	10.0 CRITICAL
CVE-2026-83021	10.0 CRITICAL
CVE-2026-83022	7.9 HIGH
CVE-2026-83023	8.6 HIGH
CVE-2026-83024	7.8 HIGH

CWE's

CWE	Beschrijving
CWE-306	Missing Authentication for Critical Function
CWE-502	Deserialization of Untrusted Data

Getroffen producten

Oracle
Helidon
Oracle Access Manager
Oracle Coherence
Oracle Data Integrator
Oracle Forms
Oracle Fusion Middleware Control
Oracle Identity Manager
Oracle Identity Manager Connector
Oracle Internet Directory
Oracle JDeveloper
Oracle Managed File Transfer
Oracle Middleware Common Libraries and Tools
Oracle Platform Security for Java
Oracle Web Services Manager
Oracle WebCenter Content

Oracle WebCenter Enterprise Capture
Oracle WebCenter Portal
Oracle WebCenter Sites
Oracle WebLogic Server
Service Delivery Platform
access_manager
webcenter_sites

Disclaimer