



NCSC-2026-0207

Kwetsbaarheden verholpen in Oracle Fusion Middleware 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 meerdere kwetsbaarheden verholpen in verschillende producten binnen de Oracle Fusion Middleware suite, waaronder WebLogic Server, WebCenter Content, WebCenter Sites, WebCenter Portal, WebCenter Enterprise Capture, Identity Manager, Identity Manager Connector, Access Manager, Coherence, Unified Directory, Virtual Directory en Application Development Framework (ADF).

Duiding

De kwetsbaarheden betreffen diverse versies van Oracle Fusion Middleware producten, waarbij een aanvaller met netwerktoegang via HTTP, HTTPS, LDAP, T3, IIOP of RMI protocollen, afhankelijk van het product en de kwetsbaarheid, ongeautoriseerde acties kan uitvoeren. Deze acties omvatten onder andere volledige systeemcompromittering, remote code execution, ongeautoriseerde creatie, wijziging of verwijdering van kritieke data, en het omzeilen van authenticatie. Sommige kwetsbaarheden vereisen gebruikersinteractie, terwijl andere kunnen worden misbruikt door ongeauthenticeerde aanvallers. De kwetsbaarheden beïnvloeden de vertrouwelijkheid, integriteit en beschikbaarheid van de getroffen systemen. Specifieke componenten zoals WebLogic Server Console, Identity Manager Connector, Access Manager Authentication Engine, en Coherence zijn ook getroffen. De CVSS 3.1 basis scores variëren van matig (rond 4.1) tot kritisch (10.0), afhankelijk van de kwetsbaarheid en het product. Exploitatie kan leiden tot volledige overname van systemen en kan impact hebben op andere Oracle producten die afhankelijk zijn van de kwetsbare componenten.

Oplossingen

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

Referenties

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

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-46788	8.4 HIGH
➤ CVE-2026-46789	9.6 CRITICAL
➤ CVE-2026-46790	5.3 MEDIUM

> CVE-2026-46791	7.5 HIGH
> CVE-2026-46792	9.9 CRITICAL
> CVE-2026-46793	9.9 CRITICAL
> CVE-2026-46794	9.9 CRITICAL
> CVE-2026-46795	9.3 CRITICAL
> CVE-2026-46796	8.0 HIGH
> CVE-2026-46797	9.8 CRITICAL
> CVE-2026-46798	10.0 CRITICAL
> CVE-2026-46799	9.8 CRITICAL
> CVE-2026-46800	10.0 CRITICAL
> CVE-2026-46801	9.8 CRITICAL
> CVE-2026-46802	9.9 CRITICAL
> CVE-2026-46803	10.0 CRITICAL
> CVE-2026-46804	8.7 HIGH
> CVE-2026-46805	9.3 CRITICAL
> CVE-2026-46806	8.2 HIGH
> CVE-2026-46807	9.8 CRITICAL
> CVE-2026-46808	8.7 HIGH
> CVE-2026-46809	9.1 CRITICAL
> CVE-2026-46810	6.5 MEDIUM
> CVE-2026-46812	6.1 MEDIUM
> CVE-2026-46813	9.8 CRITICAL
> CVE-2026-46814	9.9 CRITICAL

> CVE-2026-46838	9.9 CRITICAL
> CVE-2026-46844	9.9 CRITICAL
> CVE-2026-46845	9.8 CRITICAL
> CVE-2026-46846	10.0 CRITICAL
> CVE-2026-46847	9.9 CRITICAL
> CVE-2026-46848	7.9 HIGH
> CVE-2026-35258	8.7 HIGH
> CVE-2026-35259	8.8 HIGH
> CVE-2026-35261	6.5 MEDIUM
> CVE-2026-35262	8.3 HIGH
> CVE-2026-35263	9.9 CRITICAL
> CVE-2026-35265	8.8 HIGH
> CVE-2026-35267	8.8 HIGH
> CVE-2026-35268	9.9 CRITICAL
> CVE-2026-35269	7.5 HIGH
> CVE-2026-35270	9.1 CRITICAL
> CVE-2026-35280	9.9 CRITICAL
> CVE-2026-35281	9.9 CRITICAL
> CVE-2026-35282	9.9 CRITICAL
> CVE-2026-35283	9.9 CRITICAL
> CVE-2026-35284	9.9 CRITICAL
> CVE-2026-35285	9.9 CRITICAL
> CVE-2026-35286	9.8 CRITICAL

> CVE-2026-35291	6.6 MEDIUM
> CVE-2026-35292	10.0 CRITICAL
> CVE-2026-35293	9.8 CRITICAL
> CVE-2026-35294	9.9 CRITICAL
> CVE-2026-35295	7.5 HIGH
> CVE-2026-35296	9.8 CRITICAL
> CVE-2026-35298	9.1 CRITICAL
> CVE-2026-35299	8.8 HIGH
> CVE-2026-35300	9.8 CRITICAL
> CVE-2026-35301	10.0 CRITICAL
> CVE-2026-35302	8.3 HIGH
> CVE-2026-35303	8.8 HIGH
> CVE-2026-35304	9.8 CRITICAL
> CVE-2026-35305	9.3 CRITICAL
> CVE-2026-35306	9.3 CRITICAL
> CVE-2026-35307	10.0 CRITICAL
> CVE-2026-35308	10.0 CRITICAL
> CVE-2026-35309	9.8 CRITICAL
> CVE-2026-35310	9.8 CRITICAL
> CVE-2026-35311	8.8 HIGH
> CVE-2026-35312	9.8 CRITICAL
> CVE-2026-35313	9.9 CRITICAL
> CVE-2026-35314	7.3 HIGH

> CVE-2026-35315	8.8 HIGH
> CVE-2026-35316	9.9 CRITICAL
> CVE-2026-35317	8.8 HIGH
> CVE-2026-35318	8.8 HIGH
> CVE-2026-35319	9.8 CRITICAL
> CVE-2026-35320	9.0 CRITICAL
> CVE-2026-35321	9.9 CRITICAL
> CVE-2026-35322	8.8 HIGH
> CVE-2026-35323	9.9 CRITICAL
> CVE-2026-35324	8.8 HIGH
> CVE-2026-35325	8.8 HIGH
> CVE-2026-35326	7.2 HIGH
> CVE-2026-35327	7.6 HIGH
> CVE-2026-46765	9.9 CRITICAL
> CVE-2026-46766	9.8 CRITICAL
> CVE-2026-46767	9.9 CRITICAL
> CVE-2026-46769	7.2 HIGH
> CVE-2026-46770	6.1 MEDIUM
> CVE-2026-46771	4.1 MEDIUM
> CVE-2026-46772	4.7 MEDIUM
> CVE-2026-46773	9.8 CRITICAL
> CVE-2026-46774	9.8 CRITICAL
> CVE-2026-46776	8.6 HIGH

> CVE-2026-46777	9.1 CRITICAL
> CVE-2026-46778	10.0 CRITICAL
> CVE-2026-46779	9.9 CRITICAL
> CVE-2026-46780	8.8 HIGH
> CVE-2026-46781	10.0 CRITICAL
> CVE-2026-46782	9.9 CRITICAL
> CVE-2026-46783	9.8 CRITICAL
> CVE-2026-46784	9.1 CRITICAL
> CVE-2026-46785	9.3 CRITICAL
> CVE-2026-46786	9.6 CRITICAL
> CVE-2026-46787	8.0 HIGH

CWE's

CWE	Beschrijving
> CVE-285	Improper Authorization

Getroffen producten

Oracle
Identity Manager
Identity Manager Connector
Oracle Access Manager
Oracle Application Development Framework (ADF)

Oracle Coherence
Oracle Data Integrator
Oracle Unified Directory
Oracle Virtual Directory
Oracle WebCenter Content
Oracle WebCenter Enterprise Capture
Oracle WebCenter Portal
Oracle WebCenter Sites
WebCenter Content: Imaging
WebLogic Server

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.