Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0501

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Oracle Fusion Middleware

Publicatiedatum: 18-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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 de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Oracle heeft meerdere kwetsbaarheden verholpen in verschillende Fusion Middleware producten, waaronder Oracle WebLogic Server, Oracle Access Manager, Oracle WebCenter Portal, Oracle Application Development Framework (ADF), Oracle Fusion Middleware, Oracle Service Bus, Oracle Identity Manager Connector, Oracle Business Process Management Suite, Oracle WebCenter Content, Oracle WebCenter Sites, en Oracle Platform Security voor Java.

Duiding

De kwetsbaarheden betreffen onder andere onbevoegde toegang, manipulatie van kritieke data, denial-of-service, en remote code execution. Aanvallers kunnen via netwerktoegang, vaak zonder authenticatie, systemen volledig overnemen, data lezen, wijzigen of verwijderen, en systemen laten crashen of vastlopen. Specifieke aanvalsvectoren omvatten HTTP, SOAP, RMI, LDAP, T3, IIOP, en TLS-handshakes. Sommige kwetsbaarheden vereisen gebruikersinteractie, andere niet. Diverse componenten zoals Oracle WebLogic Server's TopLink Integration, Oracle Access Manager's Authentication Engine, Oracle Fusion Middleware's Service Delivery Platform, en Oracle Identity Manager Connector zijn getroffen. Daarnaast zijn er kwetsbaarheden in onderliggende bibliotheken zoals Bouncy Castle en Apache HttpComponents die in Oracle producten worden gebruikt.

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/cspunov2026.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-8763	9.3 CRITICAL
CVE-2026-9545	7.5 HIGH
CVE-2026-49844	6.3 MEDIUM
CVE-2026-54428	7.5 HIGH
CVE-2026-59649	8.7 HIGH
CVE-2026-64607	7.5 HIGH
CVE-2026-75596	8.7 HIGH
CVE-2026-91403	9.1 CRITICAL
CVE-2026-91416	5.9 MEDIUM
CVE-2026-91456	9.8 CRITICAL
CVE-2026-91469	9.4 CRITICAL
CVE-2026-91470	9.8 CRITICAL
CVE-2026-91498	7.2 HIGH
CVE-2026-91500	10.0 CRITICAL
CVE-2026-91507	9.3 CRITICAL
CVE-2026-91510	10.0 CRITICAL
CVE-2026-91516	7.5 HIGH
CVE-2026-91525	6.8 MEDIUM
CVE-2026-91529	6.5 MEDIUM
CVE-2026-91531	7.2 HIGH
CVE-2026-91533	8.2 HIGH
CVE-2026-91540	7.3 HIGH
CVE-2026-91543	8.2 HIGH
CVE-2026-91544	6.1 MEDIUM
CVE-2026-91548	8.6 HIGH
CVE-2026-91551	7.5 HIGH
CVE-2026-91558	8.3 HIGH
CVE-2026-91561	9.6 CRITICAL

CVE	CVSS Score
CVE-2026-91564	7.5 HIGH
CVE-2026-91566	8.8 HIGH
CVE-2026-91567	6.5 MEDIUM
CVE-2026-91569	10.0 CRITICAL
CVE-2026-91570	9.8 CRITICAL
CVE-2026-91571	6.8 MEDIUM
CVE-2026-91572	5.3 MEDIUM
CVE-2026-91575	6.8 MEDIUM
CVE-2026-91578	6.5 MEDIUM
CVE-2026-91583	9.8 CRITICAL
CVE-2026-91585	9.8 CRITICAL
CVE-2026-91586	7.4 HIGH
CVE-2026-91587	8.6 HIGH
CVE-2026-91618	9.1 CRITICAL
CVE-2026-91619	3.7 LOW
CVE-2026-91620	6.1 MEDIUM
CVE-2026-91626	6.8 MEDIUM
CVE-2026-91666	6.9 MEDIUM
CVE-2026-91667	6.5 MEDIUM
CVE-2026-91670	3.7 LOW
CVE-2026-91671	8.5 HIGH
CVE-2026-91674	3.3 LOW
CVE-2026-91675	6.5 MEDIUM
CVE-2026-91676	3.3 LOW
CVE-2026-91677	5.9 MEDIUM
CVE-2026-91678	3.3 LOW
CVE-2026-91679	3.1 LOW
CVE-2026-114823	5.4 MEDIUM
CVE-2026-114824	10.0 CRITICAL
CVE-2026-114825	8.1 HIGH
CVE-2026-114826	9.8 CRITICAL

CVE	CVSS Score
CVE-2026-114831	3.7 LOW
CVE-2026-114832	5.9 MEDIUM
CVE-2026-114833	5.3 MEDIUM
CVE-2026-114834	3.3 LOW
CVE-2026-114835	10.0 CRITICAL

CWE's

CWE	Beschrijving
CWE-116	Improper Encoding or Escaping of Output
CWE-295	Improper Certificate Validation
CWE-306	Missing Authentication for Critical Functionality
CWE-327	Use of a Broken or Risky Cryptographic Algorithm
CWE-407	Inefficient Algorithmic Complexity
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-772	Missing Release of Resource after Effective Lifetime
CWE-789	Memory Allocation with Excessive Size Value

Getroffen producten

Oracle
Construction and Engineering
Enterprise Manager
Fusion Middleware
Helidon
Oracle Access Manager

Oracle
Oracle Application Development Framework (ADF)
Oracle Autonomous Health Framework
Oracle 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.