



NCSC-2025-0334

Kwetsbaarheden verholpen in Oracle Fusion Middleware

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 21-11-2025

Revisie: 1.0.1

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

Update Revisie 1

Er is media-aandacht voor de kwetsbaarheid met kenmerk CVE-2025-61757. Verhoging in scanverkeer en potentieel misbruik wordt verwacht.

Feiten

Oracle heeft kwetsbaarheden verholpen in Oracle Fusion Middleware componenten.

Duiding

De kwetsbaarheden stellen ongeauthenticeerde aanvallers in staat om toegang te krijgen tot kritieke gegevens via HTTP, wat kan leiden tot een gedeeltelijke Denial-of-Service. De ernst van deze kwetsbaarheden wordt onderstreept door CVSS-scores van 7.5, wat wijst op aanzienlijke impact op de beschikbaarheid. Daarnaast zijn er kwetsbaarheden die kunnen leiden tot ongeautoriseerde toegang tot specifieke gegevens, met een CVSS-score van 5.3, wat duidt op een gematigd niveau van vertrouwelijkheidsimpact.

Het NCSC ontvangt berichten dat er media-aandacht is voor de kwetsbaarheid met kenmerk CVE-2025-61757. Betrouwbare partners nemen scanverkeer waar, waarin actief gezocht wordt naar mogelijke uitvoer van willekeurige code. De kwetsbaarheid bevindt zich in **Oracle Identity Manager** en betreft een issue waarbij authenticatie kan worden omzeild omdat bestanden eindigend op de extensie `.wadl` vrijgesteld zijn van authenticatie. Zomaar `.wadl` toevoegen als extensie bij een willekeurige URL zal geen effect hebben, omdat dan een niet-bestaand bestand wordt benaderd. Echter, onderzoekers hebben ontdekt dat het toevoegen van een `;` aan de extensie in theorie code-executie mogelijk kan maken.

In logging kan worden gezocht naar `;` `.wadl` als extensie. Dit duidt in elk geval op scanverkeer. Nadere analyse van de logging moet uitwijzen of uitvoer van code heeft plaatsgevonden. Op dit moment is (nog) geen indicatie ontvangen dat uitvoer van willekeurige code daadwerkelijk ergens heeft plaatsgevonden. Het NCSC kan daarom (nog) geen IoC's delen om de eigen logging te analyseren.

Het NCSC verwacht vanwege de media-aandacht en de publicatie van de onderzoekers echter wel op korte termijn een toename van scanverkeer en mogelijk werkende Proof-of-Concept-code (PoC) en adviseert de updates zo spoedig mogelijk in te zetten, indien dit (nog) niet is gebeurd.

Oplossingen

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

Referenties

➤ <https://www.oracle.com/security-alerts/cpuoct2025.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2020-15250	7.5 HIGH
➤ CVE-2023-45853	9.8 CRITICAL
➤ CVE-2024-41909	8.2 HIGH
➤ CVE-2024-48014	7.5 HIGH
➤ CVE-2025-8916	6.3 MEDIUM
➤ CVE-2025-27533	6.9 MEDIUM
➤ CVE-2025-27817	7.0 HIGH
➤ CVE-2025-48734	8.1 HIGH
➤ CVE-2025-48795	5.6 MEDIUM
➤ CVE-2025-48924	6.5 MEDIUM
➤ CVE-2025-48976	8.7 HIGH
➤ CVE-2025-53816	5.5 MEDIUM
➤ CVE-2025-55163	8.2 HIGH
➤ CVE-2025-61752	7.5 HIGH
➤ CVE-2025-61757	9.8 CRITICAL
➤ CVE-2025-61764	5.3 MEDIUM

CWE's

--

CWE	Beschrijving
➤ CWE-122	Heap-based Buffer Overflow
➤ CWE-190	Integer Overflow or Wraparound
➤ CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
➤ CWE-284	Improper Access Control
➤ CWE-306	Missing Authentication for Critical Function
➤ CWE-354	Improper Validation of Integrity Check Value
➤ CWE-400	Uncontrolled Resource Consumption
➤ CWE-404	Improper Resource Shutdown or Release
➤ CWE-674	Uncontrolled Recursion
➤ CWE-680	Integer Overflow to Buffer Overflow
➤ CWE-732	Incorrect Permission Assignment for Critical Resource
➤ CWE-770	Allocation of Resources Without Limits or Throttling
➤ CWE-787	Out-of-bounds Write
➤ CWE-789	Memory Allocation with Excessive Size Value
➤ CWE-918	Server-Side Request Forgery (SSRF)
➤ CWE-937	CWE-937
➤ CWE-1035	CWE-1035

Getroffen producten

Oracle
Identity Manager
Identity Manager (Application)
Oracle Coherence

Oracle Enterprise Data Quality
Oracle Fusion Middleware MapViewer
Oracle Global Lifecycle Management NextGen OUI Framework
Oracle JDeveloper
Oracle Middleware Common Libraries and Tools
Oracle SOA Suite
Oracle Security Service
Oracle WebCenter Forms Recognition
Oracle WebCenter Portal
Oracle WebLogic Server
Outside In Technology

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.