



NCSC-2025-0128

Kwetsbaarheden verholpen in Oracle Fusion Middleware

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 16-04-2025

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, waaronder de Utilities Application Framework, WebLogic Server, en Fusion Middleware.

Duiding

De kwetsbaarheden stellen ongeauthenticeerde kwaadwillenden in staat om toegang te krijgen tot kritieke gegevens, Denial-of-Service (DoS) te veroorzaken, en in sommige gevallen zelfs volledige controle over systemen te verkrijgen. Kwaadwillenden kunnen deze kwetsbaarheden misbruiken door speciaal vervaardigde verzoeken te sturen of door gebruik te maken van onveilige configuraties in de getroffen producten.

Oplossingen

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

Referenties

➤ <https://www.oracle.com/security-alerts/cpuapr2025.html>

Kwetsbaarheden

| CVE | CVSS Score |
|----------------------------------|--------------|
| ➤ CVE-2020-13936 | 8.8 HIGH |
| ➤ CVE-2020-25649 | 7.5 HIGH |
| ➤ CVE-2023-26464 | 9.8 CRITICAL |
| ➤ CVE-2024-7254 | 8.7 HIGH |
| ➤ CVE-2024-9143 | 6.9 MEDIUM |
| ➤ CVE-2024-11053 | 9.1 CRITICAL |
| ➤ CVE-2024-11612 | 6.9 MEDIUM |
| ➤ CVE-2024-25710 | 8.1 HIGH |

| | |
|------------------|---------------|
| ➤ CVE-2024-28168 | 6.9 MEDIUM |
| ➤ CVE-2024-29857 | 7.5 HIGH |
| ➤ CVE-2024-38476 | 9.8 CRITICAL |
| ➤ CVE-2024-40896 | 9.8 CRITICAL |
| ➤ CVE-2024-47072 | 7.7 HIGH |
| ➤ CVE-2024-47554 | 8.7 HIGH |
| ➤ CVE-2024-47561 | 9.3 CRITICAL |
| ➤ CVE-2024-50602 | 5.1 MEDIUM |
| ➤ CVE-2024-52046 | 10.0 CRITICAL |
| ➤ CVE-2024-56337 | 7.2 HIGH |
| ➤ CVE-2025-23184 | |
| ➤ CVE-2025-24970 | 6.9 MEDIUM |
| ➤ CVE-2025-27363 | 6.3 MEDIUM |

CWE's

| CWE | Beschrijving |
|------------|---|
| ➤ CVE-1336 | Improper Neutralization of Special Elements Used in a Template Engine |
| ➤ CVE-367 | Time-of-check Time-of-use (TOCTOU) Race Condition |
| ➤ CVE-754 | Improper Check for Unusual or Exceptional Conditions |
| ➤ CVE-125 | Out-of-bounds Read |
| ➤ CVE-404 | Improper Resource Shutdown or Release |
| ➤ CVE-829 | Inclusion of Functionality from Untrusted Control Sphere |
| ➤ CVE-94 | Improper Control of Generation of Code ('Code Injection') |
| ➤ CVE-400 | Uncontrolled Resource Consumption |

| | |
|---------------------------|--|
| ➤ CWE-502 | Deserialization of Untrusted Data |
| ➤ CWE-674 | Uncontrolled Recursion |
| ➤ CWE-611 | Improper Restriction of XML External Entity Reference |
| ➤ CWE-787 | Out-of-bounds Write |
| ➤ CWE-200 | Exposure of Sensitive Information to an Unauthorized Actor |
| ➤ CWE-121 | Stack-based Buffer Overflow |
| ➤ CWE-835 | Loop with Unreachable Exit Condition ('Infinite Loop') |
| ➤ CWE-20 | Improper Input Validation |

Getroffen producten

| |
|--|
| Oracle |
| Oracle Access Manager |
| Oracle Business Process Management Suite |
| Oracle HTTP Server |
| Oracle Managed File Transfer |
| Oracle SOA Suite |
| Oracle WebLogic Server |
| Oracle Outside In Technology |
| Oracle Coherence |
| Oracle Fusion Middleware MapViewer |

| |
|--|
| Oracle JDeveloper |
| Oracle WebCenter Forms Recognition |
| Oracle WebCenter Portal |
| Oracle Data Integrator |
| Oracle Business Activity Monitoring |
| Oracle Service Bus |
| Managed File Transfer |
| Weblogic Server |
| Outside In Technology |
| Coherence |
| Jdeveloper (Application) |
| WebCenter Portal |
| Data Integrator |

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.