



# NCSC-2026-0027

## Kwetsbaarheden verholpen in Oracle Fusion Middleware

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 21-01-2026

### **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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Feiten

Oracle heeft kwetsbaarheden verholpen in verschillende producten, waaronder Oracle HTTP Server, Oracle WebLogic Server, en Oracle Fusion Middleware.

## Duiding

De kwetsbaarheden in de Oracle producten stellen ongeauthenticeerde aanvallers in staat om toegang te krijgen tot gevoelige gegevens, Denial-of-Service (DoS) aanvallen uit te voeren, en de integriteit van systemen te compromitteren. Specifieke kwetsbaarheden omvatten onjuist beheer van HTTP-headers, ongecontroleerde recursie, en onvoldoende bufferbeperkingen, wat kan leiden tot systeemcrashes en gegevensverlies.

## Oplossingen

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

## Referenties

➤ <https://www.oracle.com/security-alerts/cpujan2026.html>

## Kwetsbaarheden

| CVE                              | CVSS Score    |
|----------------------------------|---------------|
| ➤ <a href="#">CVE-2021-45105</a> | 10.0 CRITICAL |
| ➤ <a href="#">CVE-2022-41342</a> | 7.8 HIGH      |
| ➤ <a href="#">CVE-2024-13009</a> | 7.2 HIGH      |
| ➤ <a href="#">CVE-2024-42516</a> | 7.5 HIGH      |
| ➤ <a href="#">CVE-2024-43204</a> | 7.5 HIGH      |
| ➤ <a href="#">CVE-2024-47252</a> | 7.5 HIGH      |
| ➤ <a href="#">CVE-2024-47554</a> | 8.7 HIGH      |
| ➤ <a href="#">CVE-2024-56406</a> | 6.3 MEDIUM    |

|                  |               |
|------------------|---------------|
| > CVE-2025-4949  | 6.8 MEDIUM    |
| > CVE-2025-5115  | 7.7 HIGH      |
| > CVE-2025-12383 | 9.4 CRITICAL  |
| > CVE-2025-23048 | 9.1 CRITICAL  |
| > CVE-2025-26333 | 5.9 MEDIUM    |
| > CVE-2025-31672 | 6.9 MEDIUM    |
| > CVE-2025-41248 | 7.5 HIGH      |
| > CVE-2025-41249 | 7.5 HIGH      |
| > CVE-2025-43967 | 2.0 LOW       |
| > CVE-2025-48924 | 6.5 MEDIUM    |
| > CVE-2025-48976 | 8.7 HIGH      |
| > CVE-2025-49796 | 5.3 MEDIUM    |
| > CVE-2025-53864 | 6.9 MEDIUM    |
| > CVE-2025-54571 | 6.9 MEDIUM    |
| > CVE-2025-54874 | 6.6 MEDIUM    |
| > CVE-2025-54988 | 9.3 CRITICAL  |
| > CVE-2025-55163 | 8.2 HIGH      |
| > CVE-2025-59375 | 6.9 MEDIUM    |
| > CVE-2025-66516 | 10.0 CRITICAL |
| > CVE-2026-21962 | 10.0 CRITICAL |

## CWE's

| CWE       | Beschrijving  |
|-----------|---|
| > CWE-20  | Improper Input Validation   |
| > CWE-79  | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')          |
| > CWE-94  | Improper Control of Generation of Code ('Code Injection')                                     |
| > CWE-113 | Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting') |
| > CWE-117 | Improper Output Neutralization for Logs   |
| > CWE-119 | Improper Restriction of Operations within the Bounds of a Memory Buffer                       |
| > CWE-122 | Heap-based Buffer Overflow  |
| > CWE-125 | Out-of-bounds Read  |
| > CWE-150 | Improper Neutralization of Escape, Meta, or Control Sequences                                 |
| > CWE-209 | Generation of Error Message Containing Sensitive Information                                  |
| > CWE-252 | Unchecked Return Value  |
| > CWE-284 | Improper Access Control   |
| > CWE-285 | Improper Authorization  |
| > CWE-289 | Authentication Bypass by Alternate Name   |
| > CWE-362 | Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')   |
| > CWE-400 | Uncontrolled Resource Consumption   |
| > CWE-404 | Improper Resource Shutdown or Release   |
| > CWE-457 | Use of Uninitialized Variable   |
| > CWE-476 | NULL Pointer Dereference  |
| > CWE-611 | Improper Restriction of XML External Entity Reference   |
| > CWE-674 | Uncontrolled Recursion  |
| > CWE-770 | Allocation of Resources Without Limits or Throttling  |

|            |   |
|------------|---|
| ➤ CWE-787  | Out-of-bounds Write   |
| ➤ CWE-827  | Improper Control of Document Type Definition                  |
| ➤ CWE-843  | Access of Resource Using Incompatible Type ('Type Confusion') |
| ➤ CWE-863  | Incorrect Authorization                                       |
| ➤ CWE-918  | Server-Side Request Forgery (SSRF)                            |
| ➤ CWE-937  | CWE-937   |
| ➤ CWE-1035 | CWE-1035  |

## Getroffen producten

|  |
|--|
| <b>Oracle</b>  |
| Data Integrator  |
| Fusion Middleware  |
| Identity Manager Connector                               |
| Managed File Transfer                                    |
| Oracle Business Process Management Suite                 |
| Oracle Coherence   |
| Oracle Global Lifecycle Management NextGen OUI Framework |
| Oracle HTTP Server                                       |
| Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in |

|   |
|---|
| Oracle Identity<br>Manager              |
| Oracle Outside In<br>Technology         |
| Oracle SOA<br>Suite                     |
| Oracle Security<br>Service              |
| Oracle Service<br>Bus                   |
| Oracle Unified<br>Directory             |
| Oracle WebCenter<br>Enterprise Capture  |
| Oracle WebLogic<br>Server               |
| Oracle Weblogic Server<br>Proxy Plug-in |
| Service Delivery<br>Platform            |
| WebCenter<br>Sites                      |

## 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.