



# NCSC-2024-0417

## Kwetsbaarheden verholpen in Oracle Fusion Middleware

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 17-10-2024

**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 Fusion Middleware componenten, zoals WebLogic Server, WebCenter en HTTP Server.

## Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Denial-of-Service (DoS)
- Manipuleren van data
- Uitvoer van willekeurige code (Administratorrechten)
- Toegang tot gevoelige gegevens

Omdat deze kwetsbaarheden zich bevinden in diverse Middleware producten, is niet uit te sluiten dat applicaties, draaiende op platformen ondersteund door deze middleware ook kwetsbaar zijn, danwel gevoelig voor misbruik van deze kwetsbaarheden.

## Oplossingen

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

## Referenties

➤ <https://www.oracle.com/security-alerts/cpuoct2024.html>

## Kwetsbaarheden

CVE	CVSS Score
➤ <a href="#">CVE-2020-11023</a>	6.9 MEDIUM
➤ <a href="#">CVE-2020-17521</a>	5.5 MEDIUM
➤ <a href="#">CVE-2022-1471</a>	
➤ <a href="#">CVE-2023-4759</a>	8.8 HIGH
➤ <a href="#">CVE-2023-35116</a>	7.1 HIGH

> CVE-2023-39743	5.3 MEDIUM
> CVE-2023-51775	7.5 HIGH
> CVE-2024-2511	7.5 HIGH
> CVE-2024-6345	
> CVE-2024-21190	7.5 HIGH
> CVE-2024-21191	7.6 HIGH
> CVE-2024-21192	
> CVE-2024-21205	
> CVE-2024-21215	7.5 HIGH
> CVE-2024-21216	9.8 CRITICAL
> CVE-2024-21234	7.5 HIGH
> CVE-2024-21246	
> CVE-2024-21260	7.5 HIGH
> CVE-2024-21274	7.5 HIGH
> CVE-2024-22201	7.5 HIGH
> CVE-2024-22262	8.1 HIGH
> CVE-2024-23807	8.1 HIGH
> CVE-2024-24549	7.5 HIGH
> CVE-2024-25269	7.5 HIGH
> CVE-2024-28182	7.5 HIGH
> CVE-2024-28752	9.3 CRITICAL
> CVE-2024-29131	7.3 HIGH
> CVE-2024-36052	7.5 HIGH

[> CVE-2024-38999](#)**10.0 CRITICAL**[> CVE-2024-45492](#)**9.8 CRITICAL**

## CWE's

CWE	Beschrijving
<a href="#">&gt; CVE-1325</a>	Improperly Controlled Sequential Memory Allocation
<a href="#">&gt; CVE-390</a>	Detection of Error Condition Without Action
<a href="#">&gt; CVE-59</a>	Improper Link Resolution Before File Access ('Link Following')
<a href="#">&gt; CVE-178</a>	Improper Handling of Case Sensitivity
<a href="#">&gt; CVE-601</a>	URL Redirection to Untrusted Site ('Open Redirect')
<a href="#">&gt; CVE-190</a>	Integer Overflow or Wraparound
<a href="#">&gt; CVE-404</a>	Improper Resource Shutdown or Release
<a href="#">&gt; CVE-1321</a>	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')
<a href="#">&gt; CVE-416</a>	Use After Free
<a href="#">&gt; CVE-401</a>	Missing Release of Memory after Effective Lifetime
<a href="#">&gt; CVE-94</a>	Improper Control of Generation of Code ('Code Injection')
<a href="#">&gt; CVE-400</a>	Uncontrolled Resource Consumption
<a href="#">&gt; CVE-770</a>	Allocation of Resources Without Limits or Throttling
<a href="#">&gt; CVE-502</a>	Deserialization of Untrusted Data
<a href="#">&gt; CVE-918</a>	Server-Side Request Forgery (SSRF)
<a href="#">&gt; CVE-787</a>	Out-of-bounds Write
<a href="#">&gt; CVE-200</a>	Exposure of Sensitive Information to an Unauthorized Actor
<a href="#">&gt; CVE-20</a>	Improper Input Validation
<a href="#">&gt; CVE-79</a>	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

## Getroffen producten

<b>oracle</b>
outside_in_technology
weblogic_server_proxy_plugin
weblogic_server
webcenter_content
webcenter_enterprise_capture
webcenter_forms_recognition
webcenter_portal
webcenter_sites_support_tools
webcenter_sites
data_integrator
business_activity_monitoring__bam_
business_activity_monitoring
business_process_management_suite
middleware_common_libraries_and_tools
enterprise_manager_fusion_middleware_control
global_lifecycle_management_fmws_installer
http_server
managed_file_transfer
identity_manager_connector

## 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.