



Advisory NCSC-2026-0448

PRIORITEIT: HOOG

Kwetsbaarheden verholpen in Oracle Fusion Middleware

Publicatiedatum: 22-10-2026

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 delen. 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 diverse producten, waaronder Oracle SOA Suite, Oracle WebLogic Server, Oracle Data Integrator, Oracle Identity Manager, Oracle Access Manager, Oracle WebCenter Content, Oracle Fusion Middleware (inclusief Helidon) en Oracle HTTP Server.

Duiding

De kwetsbaarheden betreffen onder andere onveilige deserialisatie, onvoldoende authenticatie- en toegangscontroles, kwetsbaarheden in netwerkprotocollen zoals HTTP, HTTP/2, SOAP, T3, IIOP en LDAP, en fouten in cryptografische bibliotheken zoals Bouncy Castle en Jackson-databind. Aanvallers kunnen hierdoor onder meer:

- Arbitrary code execution uitvoeren via crafted input of deserialisatieprocessen.
- Volledige systeemcompromittering bereiken via netwerktoegang zonder authenticatie.
- Ongeautoriseerde toegang verkrijgen tot gevoelige of kritieke data.
- Data manipuleren, creëren, verwijderen of wijzigen zonder juiste rechten.
- Denial-of-Service veroorzaken door resource-uitputting, crashes of hangs.
- Privilege escalation uitvoeren binnen het systeem.
- Cross-site scripting en spoofing aanvallen uitvoeren.
- Kwetsbaarheden in authenticatie- en autorisatiemechanismen misbruiken.

De kwetsbaarheden zijn aanwezig in specifieke versies van de genoemde Oracle producten en sommige onderliggende open source componenten die Oracle gebruikt. Exploitatie kan plaatsvinden via netwerktoegang, vaak zonder authenticatie, en in sommige gevallen is gebruikersinteractie vereist. Diverse kwetsbaarheden hebben een CVSS score tot 10.0, wat duidt op een hoog potentieel impactniveau. Er is (nog) geen specifieke proof-of-concept-code (PoC) bekend, maar de aard van de kwetsbaarheden maakt exploitatie mogelijk via gerichte netwerkverzoeken of gemanipuleerde data en het NCSC verwacht, vanwege de wijde verspreiding van deze producten, op korte termijn een toename in scan- en misbruikverkeer.

Oplossingen

Oracle heeft updates en patches uitgebracht voor de getroffen producten om de beschreven kwetsbaarheden te verhelpen. Gebruikers van de genoemde Oracle producten wordt geadviseerd de beschikbare updates te installeren om de beveiliging van hun systemen te waarborgen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://www.oracle.com/security-alerts/cpuoct2026.html>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-54513	8.1 HIGH
CVE-2026-56741	7.5 HIGH
CVE-2026-59649	8.7 HIGH
CVE-2026-59889	8.1 HIGH
CVE-2026-64607	7.5 HIGH
CVE-2026-83379	8.7 HIGH
CVE-2026-83396	9.8 CRITICAL
CVE-2026-83397	9.8 CRITICAL
CVE-2026-83398	8.2 HIGH
CVE-2026-83399	9.8 CRITICAL
CVE-2026-83401	6.1 MEDIUM
CVE-2026-83402	8.8 HIGH
CVE-2026-83403	8.8 HIGH
CVE-2026-83407	8.6 HIGH
CVE-2026-83409	8.1 HIGH
CVE-2026-83426	8.7 HIGH
CVE-2026-87251	9.8 CRITICAL

CVE	CVSS Score
CVE-2026-87296	7.5 HIGH
CVE-2026-87298	6.5 MEDIUM
CVE-2026-87299	6.1 MEDIUM
CVE-2026-87300	8.7 HIGH
CVE-2026-87302	9.1 CRITICAL
CVE-2026-87304	8.6 HIGH
CVE-2026-87334	5.5 MEDIUM
CVE-2026-87337	10.0 CRITICAL
CVE-2026-87346	8.7 HIGH
CVE-2026-87347	9.6 CRITICAL
CVE-2026-87359	8.8 HIGH
CVE-2026-87360	5.3 MEDIUM
CVE-2026-87361	4.3 MEDIUM
CVE-2026-87364	8.8 HIGH
CVE-2026-87365	6.5 MEDIUM
CVE-2026-87369	7.5 HIGH
CVE-2026-87370	6.5 MEDIUM
CVE-2026-87371	6.8 MEDIUM
CVE-2026-87372	6.5 MEDIUM
CVE-2026-87373	6.5 MEDIUM
CVE-2026-87374	6.8 MEDIUM
CVE-2026-87375	6.5 MEDIUM
CVE-2026-87376	6.8 MEDIUM
CVE-2026-87377	6.8 MEDIUM
CVE-2026-87378	6.5 MEDIUM
CVE-2026-87379	4.3 MEDIUM
CVE-2026-87390	5.4 MEDIUM
CVE-2026-87391	5.5 MEDIUM
CVE-2026-87392	6.5 MEDIUM
CVE-2026-87393	6.5 MEDIUM
CVE-2026-87394	8.2 HIGH

CVE	CVSS Score
CVE-2026-87395	7.5 HIGH
CVE-2026-87396	6.5 MEDIUM
CVE-2026-87397	8.8 HIGH
CVE-2026-87398	7.5 HIGH
CVE-2026-91342	8.2 HIGH
CVE-2026-91343	8.6 HIGH
CVE-2026-91344	7.5 HIGH
CVE-2026-91345	7.5 HIGH
CVE-2026-91346	8.2 HIGH
CVE-2026-91349	7.5 HIGH
CVE-2026-91350	7.5 HIGH
CVE-2026-91351	6.1 MEDIUM
CVE-2026-91352	5.3 MEDIUM
CVE-2026-91353	8.6 HIGH
CVE-2026-91354	9.9 CRITICAL
CVE-2026-91355	8.4 HIGH
CVE-2026-91358	8.2 HIGH
CVE-2026-91404	4.0 MEDIUM
CVE-2026-91405	7.5 HIGH
CVE-2026-91406	7.5 HIGH
CVE-2026-91407	8.8 HIGH
CVE-2026-91408	9.8 CRITICAL
CVE-2026-91419	7.8 HIGH
CVE-2026-91457	7.8 HIGH
CVE-2026-91458	7.8 HIGH
CVE-2026-91459	7.8 HIGH
CVE-2026-91460	7.8 HIGH
CVE-2026-91467	6.6 MEDIUM
CVE-2026-91473	7.8 HIGH
CVE-2026-91475	6.6 MEDIUM
CVE-2026-91483	7.8 HIGH

CVE	CVSS Score
CVE-2026-91488	7.1 HIGH
CVE-2026-91489	7.1 HIGH
CVE-2026-91490	9.1 CRITICAL
CVE-2026-91491	9.8 CRITICAL
CVE-2026-91492	8.7 HIGH
CVE-2026-91493	7.5 HIGH
CVE-2026-91494	7.4 HIGH
CVE-2026-91495	9.8 CRITICAL
CVE-2026-91501	5.5 MEDIUM
CVE-2026-91502	7.3 HIGH
CVE-2026-91504	7.5 HIGH
CVE-2026-91536	5.0 MEDIUM
CVE-2026-91542	7.5 HIGH
CVE-2026-91552	7.5 HIGH
CVE-2026-91616	3.7 LOW
CVE-2026-91617	5.5 MEDIUM
CVE-2026-91668	8.8 HIGH
CVE-2026-91776	7.5 HIGH
CVE-2026-101497	4.3 MEDIUM
CVE-2026-101499	9.8 CRITICAL
CVE-2026-101515	5.9 MEDIUM
CVE-2026-101520	7.5 HIGH
CVE-2026-101568	5.3 MEDIUM
CVE-2026-101569	6.5 MEDIUM
CVE-2026-101570	3.7 LOW
CVE-2026-101571	5.6 MEDIUM
CVE-2026-101572	7.5 HIGH
CVE-2026-101573	6.8 MEDIUM
CVE-2026-101574	6.9 MEDIUM
CVE-2026-101575	6.5 MEDIUM
CVE-2026-101576	3.7 LOW

CVE	CVSS Score
CVE-2026-101577	3.1 LOW
CVE-2026-101578	5.3 MEDIUM
CVE-2026-101579	7.2 HIGH
CVE-2026-101580	5.8 MEDIUM
CVE-2026-101581	6.5 MEDIUM
CVE-2026-101582	5.8 MEDIUM
CVE-2026-101583	7.0 HIGH
CVE-2026-101584	6.5 MEDIUM
CVE-2026-101585	7.2 HIGH
CVE-2026-101586	5.3 MEDIUM
CVE-2026-101587	5.3 MEDIUM
CVE-2026-101588	5.3 MEDIUM
CVE-2026-101590	9.1 CRITICAL
CVE-2022-1471	9.8 CRITICAL
CVE-2023-43622	7.5 HIGH
CVE-2024-41311	8.1 HIGH
CVE-2025-7962	6.0 MEDIUM
CVE-2026-4176	9.8 CRITICAL
CVE-2026-5598	9.9 CRITICAL
CVE-2026-8763	9.3 CRITICAL
CVE-2026-9563	7.5 HIGH
CVE-2026-12817	8.7 HIGH
CVE-2026-34477	6.3 MEDIUM
CVE-2026-41635	9.8 CRITICAL
CVE-2026-41855	8.1 HIGH
CVE-2026-42404	7.2 HIGH
CVE-2026-42779	9.8 CRITICAL
CVE-2026-47065	9.8 CRITICAL
CVE-2026-49844	6.3 MEDIUM
CVE-2026-54399	7.5 HIGH
CVE-2026-54428	7.5 HIGH

CVE	CVSS Score
CVE-2026-87399	6.3 MEDIUM
CVE-2026-87400	6.9 MEDIUM
CVE-2026-87419	8.8 HIGH
CVE-2026-87420	8.8 HIGH
CVE-2026-91210	6.5 MEDIUM
CVE-2026-91211	8.7 HIGH
CVE-2026-91212	8.6 HIGH
CVE-2026-91213	8.8 HIGH
CVE-2026-91214	9.8 CRITICAL
CVE-2026-91215	8.8 HIGH
CVE-2026-91216	10.0 CRITICAL
CVE-2026-91217	8.6 HIGH
CVE-2026-91218	9.6 CRITICAL
CVE-2026-91219	8.6 HIGH
CVE-2026-91220	9.8 CRITICAL
CVE-2026-91221	10.0 CRITICAL
CVE-2026-91222	9.9 CRITICAL
CVE-2026-91223	8.8 HIGH
CVE-2026-91224	9.9 CRITICAL
CVE-2026-91225	9.1 CRITICAL
CVE-2026-91226	7.5 HIGH
CVE-2026-91227	7.5 HIGH
CVE-2026-91228	7.1 HIGH
CVE-2026-91229	7.5 HIGH
CVE-2026-91230	9.3 CRITICAL
CVE-2026-91231	10.0 CRITICAL
CVE-2026-91232	9.9 CRITICAL
CVE-2026-91233	9.8 CRITICAL
CVE-2026-91234	9.8 CRITICAL
CVE-2026-91235	9.8 CRITICAL
CVE-2026-91236	9.8 CRITICAL

CVE	CVSS Score
CVE-2026-91237	7.5 HIGH
CVE-2026-91238	7.1 HIGH
CVE-2026-91239	8.8 HIGH
CVE-2026-91240	5.9 MEDIUM
CVE-2026-91243	9.6 CRITICAL
CVE-2026-91245	6.5 MEDIUM
CVE-2026-91246	6.1 MEDIUM
CVE-2026-91247	5.9 MEDIUM
CVE-2026-91248	5.3 MEDIUM
CVE-2026-91250	9.9 CRITICAL
CVE-2026-91251	9.9 CRITICAL
CVE-2026-91259	8.8 HIGH
CVE-2026-91261	3.1 LOW
CVE-2026-91262	5.4 MEDIUM
CVE-2026-91317	5.9 MEDIUM
CVE-2026-91318	6.5 MEDIUM
CVE-2026-91319	5.9 MEDIUM
CVE-2026-91320	5.7 MEDIUM
CVE-2026-91322	3.3 LOW
CVE-2026-91323	9.8 CRITICAL
CVE-2026-91340	8.8 HIGH
CVE-2026-91341	9.1 CRITICAL

CWE's

CWE	Beschrijving
CWE-116	Improper Encoding or Escaping of Output
CWE-125	Out-of-bounds Read
CWE-147	Improper Neutralization of Input Terminators
CWE-184	Incomplete List of Disallowed Inputs
CWE-295	Improper Certificate Validation
CWE-297	Improper Validation of Certificate with Host Mismatch
CWE-306	Missing Authentication for Critical Function
CWE-353	Missing Support for Integrity Check
CWE-354	Improper Validation of Integrity Check Value
CWE-385	Covert Timing Channel
CWE-502	Deserialization of Untrusted Data
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-772	Missing Release of Resource after Effective Lifetime
CWE-787	Out-of-bounds Write
CWE-789	Memory Allocation with Excessive Size Value
CWE-863	Incorrect Authorization
CWE-915	Improperly Controlled Modification of Dynamically-Determined Object Attributes
CWE-918	Server-Side Request Forgery (SSRF)
CWE-1104	Use of Unmaintained Third Party Components
CWE-1395	Dependency on Vulnerable Third-Party Component

Getroffen producten

Oracle
Access Manager
Business Process Management Suite
Coherence
Data Integrator
Fusion Middleware
Fusion Middleware Common Libraries And Tools
Fusion Middleware Control
Fusion Middleware MapViewer
Global Lifecycle Management NextGen OUI Framework
HTTP Server
Helidon
Identity Manager
Identity Manager (Application)
Identity Manager Connector
JDeveloper
Managed File Transfer
Middleware Common Libraries and Tools
Oracle Outside In Technology
SOA Suite
Service Bus
Web Services Manager
WebCenter Content
WebCenter Sites
WebLogic
WebLogic Server
Weblogic Server Proxy Plug-in

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 or 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.