Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0027

Kwetsbaarheden verholpen in Oracle Fusion Middleware

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 22-01-2025

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 zijn producten, waaronder Oracle Fusion Middleware, Oracle WebLogic Server, en Oracle HTTP Server.

Duiding

De kwetsbaarheden bevinden zich in verschillende Oracle producten, waaronder Oracle WebLogic Server versies 12.2.1.4.0 en 14.1.1.0.0, die het mogelijk maken voor ongeauthenticeerde kwaadwillenden om toegang te krijgen tot kritieke gegevens. Dit kan leiden tot ernstige gevolgen voor de vertrouwelijkheid, integriteit en beschikbaarheid van de systemen. De kwetsbaarheid in Oracle HTTP Server versie 12.2.1.4.0 stelt kwaadwillenden in staat om ongeautoriseerde toegang te verkrijgen, met een CVSS-score van 5.3, terwijl de kwetsbaarheid in WebLogic Server een CVSS-score van 9.8 heeft, wat wijst op een kritieke impact. Kwaadwillenden kunnen ook gebruik maken van kwetsbaarheden in Oracle Fusion Middleware en andere producten om Denial-of-Service (DoS) aanvallen uit te voeren.

Oplossingen

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

Referenties

- https://www.oracle.com/security-alerts/cpujan2025.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2019-12415	5.5 MEDIUM
CVE-2023-7272	8.6 HIGH
CVE-2023-38709	9.1 CRITICAL
CVE-2023-39410	7.5 HIGH
CVE-2023-44483	6.5 MEDIUM
CVE-2023-49582	5.5 MEDIUM

CVE-2023-51775	7.5 HIGH
CVE-2024-5535	9.1 CRITICAL
CVE-2024-6119	9.1 CRITICAL
CVE-2024-8096	7.5 HIGH
CVE-2024-23635	6.1 MEDIUM
CVE-2024-29857	7.5 HIGH
CVE-2024-30171	7.5 HIGH
CVE-2024-30172	7.5 HIGH
CVE-2024-34447	7.5 HIGH
CVE-2024-34750	7.5 HIGH
CVE-2024-37370	9.1 CRITICAL
CVE-2024-37371	9.1 CRITICAL
CVE-2024-38473	9.1 CRITICAL
CVE-2024-38475	9.1 CRITICAL
CVE-2024-38816	8.1 HIGH
CVE-2024-38819	7.5 HIGH
CVE-2024-38998	9.8 CRITICAL
CVE-2024-38999	10.0 CRITICAL
CVE-2024-40898	9.1 CRITICAL
CVE-2024-45490	9.8 CRITICAL
CVE-2024-45491	9.8 CRITICAL
CVE-2024-45492	9.8 CRITICAL
CVE-2024-47072	7.5 HIGH

CVE-2024-47554	7.5 HIGH
CVE-2024-47561	9.8 CRITICAL
CVE-2025-21498	5.3 MEDIUM
CVE-2025-21535	9.8 CRITICAL
CVE-2025-21549	7.5 HIGH

CWE's

CWE	Beschrijving
CWE-338	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)
CWE-35	Path Traversal: '.../...//'
CWE-1395	Dependency on Vulnerable Third-Party Component
CWE-130	Improper Handling of Length Parameter Inconsistency
CWE-755	Improper Handling of Exceptional Conditions
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-116	Improper Encoding or Escaping of Output
CWE-190	Integer Overflow or Wraparound
CWE-532	Insertion of Sensitive Information into Log File
CWE-798	Use of Hard-coded Credentials
CWE-125	Out-of-bounds Read
CWE-284	Improper Access Control
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-295	Improper Certificate Validation
CWE-400	Uncontrolled Resource Consumption
CWE-502	Deserialization of Untrusted Data
CWE-22	

Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	
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-122	Heap-based Buffer Overflow
CWE-121	Stack-based Buffer Overflow
CWE-20	Improper Input Validation
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

oracle
http_server
fusion_middleware_mapviewer
fusion_middleware
weblogic_server
security_service
business_activity_monitoring
business_activity_monitoring__bam_
identity_manager
managed_file_transfer
middleware_common_libraries_and_tools
business_process_management_suite
outside_in_technology
webcenter_portal

Disclaimer