Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op 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 infomatie.

Referenties

› https://www.oracle.com/security-alerts/cpuoct2024.html

Kwetsbaarheden

CVE	CVSS Score
› CVE-2020-11023	6.9 MEDIUM
› CVE-2020-17521	5.5 MEDIUM
› CVE-2022-1471	
› CVE-2023-4759	8.8 HIGH
› CVE-2023-35116	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
CWE-1325	Improperly Controlled Sequential Memory Allocation
CWE-390	Detection of Error Condition Without Action
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-178	Improper Handling of Case Sensitivity
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
CWE-190	Integer Overflow or Wraparound
CWE-404	Improper Resource Shutdown or Release
CWE-1321	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')
CWE-416	Use After Free
CWE-401	Missing Release of Memory after Effective Lifetime
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-400	Uncontrolled Resource Consumption
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-502	Deserialization of Untrusted Data
CWE-918	Server-Side Request Forgery (SSRF)
CWE-787	Out-of-bounds Write
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-20	Improper Input Validation
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

oracle
outside_in_technology
weblogic_server_proxy_plug-in
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_fmw_installer
http_server
managed_file_transfer
identity_manager_connector

Disclaimer