

CVE-2017-3506

Oracle WebLogic Server OS Command Injection Vulnerability

CISA KEV since Jun 3, 2024

Actively exploited

Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services). Supported versions that are affected are 10.3.6.0, 12.1.3.0, 12.2.1.0, 12.2.1.1 and 12.2.1.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data as well

EVRS 83/₁₀₀ Urgent priority	CVSS V3.1 7.4 High · NVD	EPSS 0.960 99.88th percentile · FIRST	CISA DEADLINE Jun 24, 2024 KEV since 2024 · listed over a year
---	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.960 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.4	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Basis: CISA KEV required action

as unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
weblogic server	10.3.6.0.0 12.1.3.0.0 12.2.1.0.0 12.2.1.1.0 12.2.1.2.0	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-2f3c-chf6-54v5
NVD nvd.nist.gov/vuln/detail/CVE-2017-3506
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2017-12627

oracle.com oracle.com/security-alerts/cpuapr2017.html
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2017-3506

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.