



# CVE-2017-3506

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#) 

## Summary

<b>CVE</b>	CVE-2017-3506
<b>State</b>	PUBLISHED
<b>Assigner</b>	oracle
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-04-24 19:59:03 UTC
<b>Updated</b>	2026-04-22 13:39:47 UTC
<b>Description</b>	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services). Suppr

## Risk And Classification

**Primary CVSS:** v3.1 7.4 HIGH from nvd@nist.gov

**CVSS:** 3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

**EPSS:** 0.943930000 probability, percentile 0.999730000 (date 2026-04-23)

**CISA KEV:** Listed on 2024-06-03; due 2024-06-24; ransomware use Unknown

**Problem Types:** NVD-CWE-noinfo | CWE-78 | 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 as unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. | CWE-78 CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.4	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N
3.1	ADP	DECLARED	7.4	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.4	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N
2.0	nvd@nist.gov	Primary	5.8		AV:N/AC:M/Au:N/C:P/I:P/A:N

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

### CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:P/I:P/A:N

### CISA Known Exploited Vulnerability

<b>Vendor</b>	Oracle
<b>Product</b>	WebLogic Server
<b>Name</b>	Oracle WebLogic Server OS Command Injection Vulnerability
<b>Required Action</b>	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
<b>Notes</b>	<a href="https://www.oracle.com/security-alerts/cpuapr2017.html">https://www.oracle.com/security-alerts/cpuapr2017.html</a> ; <a href="https://nvd.nist.gov/vuln/detail/CVE-2017-3506">https://nvd.nist.gov/vuln/detail/CVE-2017-3506</a>

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Weblogic Server	10.3.6.0.0	All	All	All

Application	Oracle	Weblogic Server	12.1.3.0.0	All	All	All
Application	Oracle	Weblogic Server	12.2.1.0.0	All	All	All
Application	Oracle	Weblogic Server	12.2.1.1.0	All	All	All
Application	Oracle	Weblogic Server	12.2.1.2.0	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Oracle Corporation	WebLogic Server	affected 10.3.6.0	Not specified
CNA	Oracle Corporation	WebLogic Server	affected 12.1.3.0	Not specified
CNA	Oracle Corporation	WebLogic Server	affected 12.2.1.0	Not specified
CNA	Oracle Corporation	WebLogic Server	affected 12.2.1.1	Not specified
CNA	Oracle Corporation	WebLogic Server	affected 12.2.1.2	Not specified
ADP	Oracle	Weblogic Server	affected 10.3.6.0.0	Not specified
ADP	Oracle	Weblogic Server	affected 12.1.3.0.0	Not specified
ADP	Oracle	Weblogic Server	affected 12.2.1.0.0	Not specified
ADP	Oracle	Weblogic Server	affected 12.2.1.1.0	Not specified
ADP	Oracle	Weblogic Server	affected 12.2.1.2.0	Not specified
ADP	Oracle	Weblogic Server	affected 10.3.6.0.0	Not specified
ADP	Oracle	Weblogic Server	affected 12.1.3.0.0	Not specified
ADP	Oracle	Weblogic Server	affected 12.2.1.0.0	Not specified
ADP	Oracle	Weblogic Server	affected 12.2.1.1.0	Not specified
ADP	Oracle	Weblogic Server	affected 12.2.1.2.0	Not specified
ADP	Oracle	Weblogic Server	affected 10.3.6.0.0	Not specified
ADP	Oracle	Weblogic Server	affected 12.1.3.0.0	Not specified
ADP	Oracle	Weblogic Server	affected 12.2.1.0.0	Not specified
ADP	Oracle	Weblogic Server	affected 12.2.1.1.0	Not specified
ADP	Oracle	Weblogic Server	affected 12.2.1.2.0	Not specified
ADP	Oracle	Weblogic Server	affected 10.3.6.0.0	Not specified
ADP	Oracle	Weblogic Server	affected 12.1.3.0.0	Not specified
ADP	Oracle	Weblogic Server	affected 12.2.1.0.0	Not specified
ADP	Oracle	Weblogic Server	affected 12.2.1.1.0	Not specified
ADP	Oracle	Weblogic Server	affected 12.2.1.2.0	Not specified
ADP	Oracle	Weblogic Server	affected 10.3.6.0.0	Not specified
ADP	Oracle	Weblogic Server	affected 12.1.3.0.0	Not specified
ADP	Oracle	Weblogic Server	affected 12.2.1.0.0	Not specified
ADP	Oracle	Weblogic Server	affected 12.2.1.1.0	Not specified

ADP	Oracle	Weblogic Server	affected 12.2.1.2.0	Not specified
-----	--------	-----------------	---------------------	---------------

## References

Reference	Source
Oracle Critical Patch Update - April 2017	af8544
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c7
Oracle WebLogic Server CVE-2017-3506 Remote Security Vulnerability	af8544
Oracle WebLogic Server Bugs Let Remote Users Access and Modify Data and Cause Denial of Service Conditions - SecurityTracker	af8544
CVE Program record	CVE.C
NVD vulnerability detail	NVD
CISA Known Exploited Vulnerabilities catalog	CISA

No vendor comments have been submitted for this CVE.

## Additional Advisory Data

Source	Time	Event
ADP	2024-06-03T00:00:00.000Z	CVE-2017-3506 added to CISA KEV

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)