CVE-2017-10271

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-10271
State	PUBLISHED
Assigner	oracle
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-19 17:29:01 UTC
Updated	2026-04-21 20:07:45 UTC
Description	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Security). Supp

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from nvd@nist.gov

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

EPSS: 0.944390000 probability, percentile 0.999890000 (date 2026-04-25)

CISA KEV: Listed on 2022-02-10; due 2022-08-10; ransomware use Known

Problem Types: NVD-CWE-noinfo | CWE-306 | Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. | CWE-306 CWE-306 Missing Authentication for Critical Function

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	ADP	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

CISA Known Exploited Vulnerability

Vendor	Oracle
Product	WebLogic Server
Name	Oracle Corporation WebLogic Server Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2017-10271

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	12.2.1.1.0	All	All	All
Application	Oracle	Weblogic Server	12.2.1.2.0	All	All	All

Application	Oracle	WebLogic Server	12.1.3.0.0	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Oracle Corporation	WebLogic Server	affected 10.3.6.0.0	Not specified
CNA	Oracle Corporation	WebLogic Server	affected 12.1.3.0.0	Not specified
CNA	Oracle Corporation	WebLogic Server	affected 12.2.1.1.0	Not specified
CNA	Oracle Corporation	WebLogic Server	affected 12.2.1.2.0	Not specified

References

Reference
Oracle WebLogic - wls-wsat Component Deserialization Remote Code Execution (Metasploit) - Multiple remote Exploit
Oracle WebLogic < 10.3.6 - 'wls-wsat' Component Deserialisation Remote Command Execution
Oracle WebLogic Server CVE-2017-10271 Remote Security Vulnerability
Oracle Critical Patch Update - October 2017
www.cisa.gov/known-exploited-vulnerabilities-catalog
GitHub - c0mmand3rOpSec/CVE-2017-10271: WebLogic Exploit
Oracle WebLogic Server Flaws Let Remote User Gain Elevated Privileges, Modify Data, and Deny Service on the Target System - SecurityTra
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-02-10T00:00:00.000Z	CVE-2017-10271 added to CISA KEV

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