

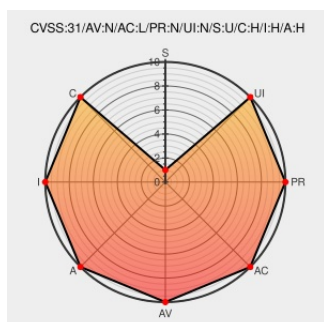


CVE-2020-14645

Published on: 07/15/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:01 PM UTC

CVE-2020-14645

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Weblogic Server](#) from [Oracle](#) contain the following vulnerability:

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server.

Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.

CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

CVE-2020-14645 has been assigned by [secalert_us@oracle.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [Oracle Corporation](#) - **WebLogic Server** version = **10.3.6.0.0**

Affected Vendor/Software: [Oracle Corporation](#) - **WebLogic Server** version = **12.1.3.0.0**

Affected Vendor/Software: [Oracle Corporation](#) - **WebLogic Server** version = **12.2.1.3.0**

Affected Vendor/Software: [Oracle Corporation](#) - **WebLogic Server** version = **12.2.1.4.0**

Affected Vendor/Software: [Oracle Corporation](#) - **WebLogic Server** version = **14.1.1.0.0**

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
---------------	-------------------	----------------

Level	Confidentiality	Integrity	Availability
Network	Low	Low	None
Confidentiality Impact	Integrity Impact	Availability Impact	
Partial	Partial	Partial	

CVE References

Description	Tags	Link
Oracle Critical Patch Update Advisory - July 2020	Vendor Advisory www.oracle.com text/html	 MISC www.oracle.com/security-alerts/cpujul2020.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

环境下载

Known Affected Configurations (CPE V2.3)

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	12.2.1.3.0	All	All	All
Application	Oracle	Weblogic Server	12.2.1.4.0	All	All	All
Application	Oracle	Weblogic Server	14.1.1.0.0	All	All	All
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	12.2.1.3.0	All	All	All
Application	Oracle	Weblogic Server	12.2.1.4.0	All	All	All
Application	Oracle	Weblogic Server	14.1.1.0.0	All	All	All
cpe:2.3:a:oracle:weblogic_server:10.3.6.0.0:*****:.*:						
cpe:2.3:a:oracle:weblogic_server:12.1.3.0.0:*****:.*:						
cpe:2.3:a:oracle:weblogic_server:12.2.1.3.0:*****:.*:						
cpe:2.3:a:oracle:weblogic_server:12.2.1.4.0:*****:.*:						
cpe:2.3:a:oracle:weblogic_server:14.1.1.0.0:*****:.*:						

cpe:2.3:a:oracle:weblogic_server:10.3.6.0.0:*****:
cpe:2.3:a:oracle:weblogic_server:12.1.3.0.0:*****:
cpe:2.3:a:oracle:weblogic_server:12.2.1.3.0:*****:
cpe:2.3:a:oracle:weblogic_server:12.2.1.4.0:*****:
cpe:2.3:a:oracle:weblogic_server:14.1.1.0.0:*****:

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
🔒 @m0rb	(ex: CVE-2020-2555, CVE-2020-2883, CVE-2020-14645)	2022-03-02 22:53:35
🔒 @buaqbot	CVE-2020-14645 Weblogic UniversalExtractor Bypass ReflectionExtractor via T3 protocol ift.tt/nDXTYiL ift.tt/mFfpqu0	2022-12-19 11:19:59