



CVE-2020-14883

Published on: 10/21/2020 12:00:00 AM UTC

Last Modified on: 07/12/2022 05:42:00 PM UTC

CVE-2020-14883

[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: Console). 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 high privileged attacker with network access via HTTP to compromise Oracle

WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).

CVE-2020-14883 has been assigned by secalert_us@oracle.com to track the vulnerability - currently rated as **HIGH** 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: **7.2 - HIGH**

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

CVSS2 Score: **9 - HIGH**

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

CONFIDENTIAL	Complexity	
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Oracle Critical Patch Update Advisory - October 2020	Vendor Advisory www.oracle.com text/html	 MISC www.oracle.com/security-alerts/cpuoct2020.html
Oracle WebLogic Server Administration Console Handle Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/160143/Oracle-WebLogic-Server-Administration-Console-Handle-Remote-Code-Execution.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

weblogic 漏洞扫描工具。目前包含对以下漏洞的检测能力：CVE-2014-4210、CVE-2016-0638、CVE-2016-3510、CVE-2017-3248、CVE-2017-3506、CVE-2017-10271、C...

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)
 @ipssignatures	It's new to me that Astaro has a protection/signature/rule for the vulnerability CVE-2020-14883.... twitter.com/i/web/status/1...	2021-11-20 22:02:02
 @ipssignatures	I know 3 other IPSs that have protections/signatures/rules for the vulnerability CVE-2020-14883. ipssignatures.appspot.com/?cve=CVE-2020-...#S3m7osrvtdiocw	2021-11-20 22:02:02
 @_nob7dy_	@alph4byt3 github.com/projectdiscover...	2022-04-06 23:30:56
 @alph4byt3	Some info regarding this. 1) This is not original, it's indeed CVE-2020-14883. 2) I found it using a custom privat... twitter.com/i/web/status/1...	2022-04-07 14:42:14
 @RemotelyAlerts	Severity: ??? Vulnerability in the Oracle WebLogic Ser... CVE-2020-14883 Link for more: alerts.remotelymmm.com/CVE-2020-14883	2022-07-01 17:30:54
 @ze2paac	Access Admin Console. هتسمحلي أعمل CVE-2020-14883 ده فيه خلاص بعد م لقيت ال... ورايح أبلغ الثغره قولت أم twitter.com/i/web/status/1...	2022-11-02 00:45:39
 /r/SecOpsDaily	ZOMiner exploit Elasticsearch and Jenkins vulnerability CVE-2015-1427 and CVE-2020-14883 for spreading botnet and mining Monero	2021-03-10 16:48:27
 /r/weblogic	Vulnerability analysis WebLogic unauthorized access and command execution analysis (CVE-2020-14882/14883)	2021-04-30 07:00:38

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#).

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