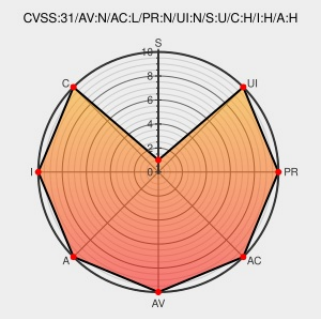
CVE-2020-14882

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

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

CVE-2020-14882

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 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. 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-2020-14882 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: 10 - HIGH

Access Vector	Access Complexity	Authentication

NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Oracle WebLogic Server 12.2.1.0 Remote Code Execution ≈ Packet Storm	Exploit, Third Party Advisory, VDB Entry, packetstormsecurity.com, text/html	MISC packetstormsecurity.com/files/161128/Oracle-WebLogic-Server-12.2.1.0-Remote-Code-Execution.html
Oracle WebLogic Server Remote Code Execution ≈ Packet Storm	Exploit, Third Party Advisory, VDB Entry, packetstormsecurity.com, text/html	MISC packetstormsecurity.com/files/159769/Oracle-WebLogic-Server-Remote-Code-Execution.html
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	Exploit, Third Party Advisory, VDB Entry, packetstormsecurity.com, text/html	MISC packetstormsecurity.com/files/160143/Oracle-WebLogic-Server-Administration-Console-Handle-Remote-Code-Execution.html

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Bash script to exploit the Oracle's Weblogic Unauthenticated Remote Command Execution - CVE-2020-14882

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)
@RapidSafeguard	Saturday with #Dork #CVE-2020-14882: #Oracle WebLogic Server Google Dork : inurl:"/console/login/LoginForm.jsp PoC… twitter.com/i/web/status/1…	2021-05-09 17:58:30
@ipssignatures	The vuln CVE-2020-14882 has a tweet created 0 days ago and retweeted 11 times. twitter.com/RapidSafeguard… #pow1rtrtwwcve	2021-05-09 23:06:00
@bishopfox	ICYMI: #Oracle #WebLogic CVE-2020-14882 remains an attractive target for would-be attackers. Ensure your software i… twitter.com/i/web/status/1…	2021-05-10 18:02:10
@TheDFIRReport	WebLogic RCE Leads to XMRig ➡Initial Access: WebLogic Unauthorized RCE CVE-2020-14882 ➡Execution: PowerShell sc… twitter.com/i/web/status/1…	2021-06-03 12:24:53
@GossiTheDog	A reminder to patch RCE CVE-2020-14882, which continues to be used in the wild twitter.com/TheDFIRReport/…	2021-06-03 12:28:57
@r00tpgp	for cve-2020: github.com/corelight/CVE-…	2021-07-23 12:36:49
@campuscodi	Targets include Linux servers vulnerable to: -CVE-2020-14882 (WebLogic) -CVE-2017-11610 (Supervisord) These attack… twitter.com/i/web/status/1…	2021-08-12 17:48:52
@ipssignatures	The vuln CVE-2020-14882 has a tweet created 0 days ago and retweeted 10 times. twitter.com/campuscodi/sta… #pow1rtrtwwcve	2021-08-13 05:06:00
@RapidSafeguard	Unauthenticated RCE CVE-2020-14882 curl -X POST 'http://target:7001/console/css/%252e%252e%252fconsole.portal'… twitter.com/i/web/status/1…	2021-09-02 20:55:38

@infinityABCDE	vulmap version 0.3 github.com/zhzyker/vulmap 新蹭 Weblogic CVE-2020-14882 新蹭 Weblogic CVE-2020-2883 新蹭 Weblogic CVE-202… twitter.com/i/web/status/1…	2021-09-16 13:06:07
@AcademicoCert	?? CVE-2020-14882 infects vía remote code execution (RCE) flaw in Oracle WebLogic Server, and CVE-2018-20062, anoth… twitter.com/i/web/status/1…	2021-09-16 14:31:40
@infinityABCDE	Oracle Weblogic PoC for vulnerabilities CVE-2020-14750 and cve-2020-14882 Be careful ! It is working ./CVE-2020-1… twitter.com/i/web/status/1…	2021-09-22 02:22:06
@secalertsasia	Among others Capoae exploits CVE-2020-14882 which is a remote code execution bug in the Oracle WebLogic Server.… twitter.com/i/web/status/1…	2021-10-04 21:39:28
@secalertsasia	Among others Capoae exploits CVE-2020-14882 which is a remote code execution bug in the Oracle WebLogic Server.… twitter.com/i/web/status/1…	2021-10-05 11:39:20
@secalertsasia	Among others Capoae exploits CVE-2020-14882 which is a remote code execution bug in the Oracle WebLogic Server.… twitter.com/i/web/status/1…	2021-10-07 03:12:23
@secalertsasia	Among others Capoae exploits CVE-2020-14882 which is a remote code execution bug in the Oracle WebLogic Server.… twitter.com/i/web/status/1…	2021-10-07 10:39:28
@secalertsasia	Among others Capoae exploits CVE-2020-14882 which is a remote code execution bug in the Oracle WebLogic Server.… twitter.com/i/web/status/1…	2021-10-07 12:39:27
@TrendMicroRSRCH	We look into campaigns that exploit the following server vulnerabilities: CVE-2021-26084, CVE-2020-14882, CVE-2020-… twitter.com/i/web/status/1…	2021-10-18 13:30:00
@TheDFIRReport	A Threat actor recently exploited a vulnerability (CVE-2020-14882) in WebLogic to drop XMRig. Exploit->exec xx.xml… twitter.com/i/web/status/1…	2021-10-21 16:45:12
@ipssignatures	The vuln CVE-2020-14882 has a tweet created 0 days ago and retweeted 11 times. twitter.com/TheDFIRReport/… #pow1rtrtwwcve	2021-10-21 20:06:00
@bad_packets	@TheDFIRReport We're also seeing CVE-2020-14882 activity from 192.3.194.202 (??) – payload has changed three times:… twitter.com/i/web/status/1…	2021-10-22 02:22:39
@AttilaDeak01	CVE-2020-14882,3 CVE-2021-42013,1	2021-10-30 17:37:06
@TheDFIRReport	We are currently seeing WebLogic exploitation (CVE-2020-14882) which leads to a XMRig miner installation. The expl… twitter.com/i/web/status/1…	2021-11-30 12:35:33
@TheDFIRReport	Detections IDS Sigs ET WEB_SPECIFIC_APPS Possible Oracle WebLogic RCE Inbound M2 (CVE-2020-14882) ET POLICY Exter… twitter.com/i/web/status/1…	2021-11-30 12:35:34
@NaibuKansa_Info	珍しく警察庁情報　→　警察庁「Oracle WebLogic Server の脆弱性（CVE-2020-14882）を標的としたアクセスの観測等について 」– 内部監査.com 内部監査.com/?p=6618 https://t.co/qsb5hcedpx	2021-12-27 09:00:02
@Alra3ees	Exphub Including exploit scripts for Webloigc, Struts2, Tomcat, Nexus, Solr, Jboss, Drupal, CVE-2020-14882, CVE-20… twitter.com/i/web/status/1…	2022-01-28 12:36:06
@h1pmnh	@alph4byt3 CVE-2020-14882?	2022-04-06 12:46:18
@TrendMicroRSRCH	NEW BLOG ENTRY: We discuss how malicious actors are abusing older #vulnerabilities such as CVE-2020-14882 to take a… twitter.com/i/web/status/1…	2022-09-16 07:00:00
@hackyseguridad	Hackers Atacando activamente Oracle WebLogic Server product of Oracle Fusion Middleware.. CVE-2020-14882, CVE-2020… twitter.com/i/web/status/1…	2022-09-16 17:34:40
@MariaRusanova88	CVE-2020-14882 CVSS score: 9.8 :: chose be patched (Oracle WebLogic Server parch) or be hacked	2022-09-19 22:56:57
@TrendMicroRSRCH	We provide a technical analysis of how malicious actors are abusing the CVE-2020-14882 #WebLogic Server… twitter.com/i/web/status/1…	2022-09-20 01:14:21
	We discuss how Trend Micro solutions effectively thwarted the abuse of the CVE-2020-14882	2022-09-23

@TrendMicroRSRCH	#WebLogic #vulnerability,… twitter.com/i/web/status/1…	14:49:00
@TrendMicroLATAM	Discutimos cómo los cibercriminales están abusando de vulnerabilidades más antiguas como CVE-2020-14882 para aprove… twitter.com/i/web/status/1…	2022-09-23 21:37:00
@TrendMicroRSRCH	We discuss how Trend Micro solutions effectively thwart the abuse of the CVE-2020-14882 #WebLogic #vulnerability in… twitter.com/i/web/status/1…	2022-09-28 01:00:00
@GossiTheDog	A reminder to patch CVE-2020-14882 in WebLogic.	2022-09-28 10:25:02
@TrendMicro	We discuss how Trend Micro solutions effectively thwarted the abuse of the CVE-2020-14882 #WebLogic #vulnerability,… twitter.com/i/web/status/1…	2022-09-29 18:00:00
@TrendMicroES	Hablamos de cómo las soluciones de Trend Micro frustraron eficazmente el abuso de la #vulnerabilidad CVE-2020-14882… twitter.com/i/web/status/1…	2022-09-30 14:00:00
@Vulnmachines	oracle weblogic #rce | CVE-2021-2109 | CVE-2020-14882 Chaining of 2 CVEs (CVE-2020-14882 + CVE-2021-2109) authentic… twitter.com/i/web/status/1…	2022-10-04 08:33:00
@Vulnmachines	CVE-2020-14882 in Weblogic - dork for Netlas.io: tag.weblogic.version:(10.3.6.0 OR 12.1.3.0 OR 12.2.… twitter.com/i/web/status/1…	2022-10-04 09:03:57
@ipssignatures	The vuln CVE-2020-14882 has a tweet created 0 days ago and retweeted 12 times. twitter.com/Vulnmachines/s… #pow1rtrtwwcve	2022-10-04 16:06:01
@TrendMicroRSRCH	We discuss how malicious actors are abusing older #vulnerabilities such as CVE-2020-14882 to take advantage of impr… twitter.com/i/web/status/1…	2022-10-05 11:00:00
@TrendMicroLATAM	Discutimos cómo las soluciones de Trend Micro detuvieron efectivamente el abuso de la vulnerabilidad CVE-2020-14882… twitter.com/i/web/status/1…	2022-10-09 16:15:00
/r/weblogic	Vulnerability analysis | WebLogic unauthorized access and command execution analysis (CVE-2020-14882/14883)	2021-04-30 07:00:38
/r/CryptoCurrency	This cryptocurrency miner is exploiting the new Confluence remote code execution bug.	2021-09-23 07:55:17

← Previous ID

Next ID→