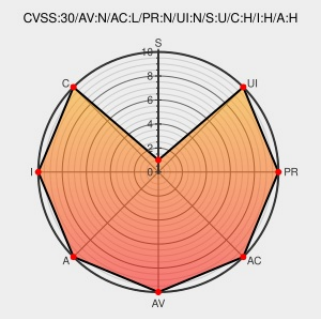
CVE-2020-2551

Published on: 01/15/2020 12:00:00 AM UTC

Last Modified on: 10/25/2022 05:59:00 PM UTC

CVE-2020-2551

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: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

CVE-2020-2551 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**

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
NETWORK	LOW	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Oracle Critical Patch Update Advisory - January 2020	Vendor Advisory www.oracle.com text/html	MISC www.oracle.com/security-alerts/cpujan2020.html

There are currently no QIDs associated with this CVE

Exploit/POC from Github

CVE-2020-2551

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	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

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: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:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@3th1c_yuk1	Anyone knows the exact exploitation of CVE-2020-2551 please attach any references !! @ADITYASHENDE17… twitter.com/i/web/status/1…	2021-05-09 18:02:52
@R007_BR34K3R	Reported 8 bugs in 6 subdomains to @NCIIPC Time based Sqli, [cve-2020-2551 (RCE) with @pdnuclei] , OpenRedirect,… twitter.com/i/web/status/1…	2021-07-28 09:25:26
@caffeinevulns	#Day15 went by trying to read more about CVE-2020-2551 and setting up proper environment for the machine to do some… twitter.com/i/web/status/1…	2021-08-17 03:47:12
@Prohacktiv3	? Surveillance des #POC (Proof Of Concept) sur @github : ? CVE-2020-2551: github.com/0xAbbarhSF/CVE… ? CVE-2022-30190… twitter.com/i/web/status/1…	2022-06-03 06:07:34
@OSINT_info	? Surveillance des #POC (Proof Of Concept) sur : ? CVE-2020-2551: github.com/0xAbbarhSF/CVE… ? CVE-2022-30190:… twitter.com/i/web/status/1…	2022-06-03 06:11:21
@AhmedMa07846126	is anyone have good poc for this CVE-2020-2551 i tried everything to make poc but i didn't :(i have 10 subdomins v… twitter.com/i/web/status/1…	2022-06-11 10:54:57
@Rooted0x01	@AhmedMa07846126 Check this medium.com/@qazbnm456/cve… POC github.com/hktalent/CVE-2… not TESTED	2022-06-11 10:59:58
@MedPyDev	Any working PoC for those CVE's "CVE-2020-2551" | CVE-2017-10271 i tried some pot from GitHub but nothing work for… twitter.com/i/web/status/1…	2022-06-28 18:25:10
@buaqbot	CVE-2020-2551 深入 IIOP 检测与 Non-Java(Yak) 利用 ift.tt/A7NtylC ift.tt/Eqn74yf	2022-07-15 10:02:18
@buaqbot	Weblogic CVE-2020-2551 绕过NAT网络分析 ift.tt/wFjqla9 ift.tt/BUwlTmr	2022-11-10 06:27:13
@CVEtrends	Top 3 trending CVEs on Twitter Past 24 hrs: CVE-2013-3900: 265.7K (audience size) CVE-2020-2551: 169.3K CVE-2023-2… twitter.com/i/web/status/1…	2023-04-02 13:00:02

← Previous ID

Next ID→