Indusface Security Bulletin

Oracle WebLogic Server Deserialization Remote Command Execution Vulnerability (CVE-2019-2725)

May 2019

What is Oracle WebLogic RCE Vulnerability (CVE-2019-2725)?

Oracle has released a security advisory on 26th of April, 2019 with an out-of-band patch fixing a critical 0day vulnerability in Oracle WebLogic Server (**CVE-2019-2725**) affecting versions 10.3.6.0 & 12.1.3.0. The vulnerability was discovered by couple of researcher groups and made public by KnownSec 404 Team on 21st of April, 2019. Exploitation of this vulnerability was surged when Proof-of-Concept (POC) was also made available to public.

Oracle WebLogic Server (part of Oracle Fusion Middleware) is a popular application server for building and deploying enterprise-ready Java Platform, Enterprise Edition (Java EE) applications.

Vulnerability exists in wls9_async_response.war package, which provides asynchronous communication for WebLogic Server service and it is included by default. The package can be misused when deserializing input data by sending a specially crafted SOAP requests with XML <work:WorkContext>, <wsa:Action>, <wsa:RelatesTo>, and <class> tags. Successful exploitation could allow an unauthenticated attacker to execute remote code and possibly gain access to a targeted system.

What are the risks?

Oracle WebLogic Server (part of Oracle Fusion Middleware) is a popular application server for building and deploying enterprise-ready Java Platform, Enterprise Edition (Java EE) applications.

According to Zoomeye.org, there are about 41,000 publicly accessible WebLogic instances currently in use. The vulnerable package wls9_async_response.war is included by default in widely-used versions of WebLogic Servers, such as 10.3.6 and 12.1.3. Multiple working POCs are already available in public and no user interaction required to exploit the vulnerability makes the exploitation easy for any remote & unauthenticated user to conduct attacks.

Active attacks are already seen and has been reported by multiple security blog posts & forums. SANS ISC InfoSec also reported that the vulnerability is being exploited in wild and are used to install crypto coin miners.

Severity: Critical

CVSSv2: Base Score 10
Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSSv3: Base Score 9.8
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Do I need to worry about it?

Vendor has released security patch and we strongly advise customers to update their installations as soon as possible.

Mitigation:

Apply Oracle's official patches for affected versions of WebLogic 10.3.6 & 12.1.3.

Find and delete wls9_async_response.war, wls-wsat.war packages and restart the Weblogic service.

Restrict/Disable URL access for /_async/* and /wls-wsat/* paths.

Indusface Web Application Scanning (WAS) performs scans on the server and it can identify this vulnerability through non-intrusive remote network test.

Indusface AppTrana/Total Application Security (TAS) platform protects against web application layer vulnerabilities being exploited by external traffic and will be able to protect this vulnerability by customized rules.