

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

04/26/2019

04/27/2019 - UPDATED

SUBJECT:

A Vulnerability in Oracle WebLogic Could Allow for Remote Code Execution

OVERVIEW:

A vulnerability has been discovered in the Oracle WebLogic that could allow for remote code execution. Oracle WebLogic is an application server used for building and hosting Java-EE applications. Successful exploitation of this vulnerability could result in remote code execution within the context of the application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

There are reports of this vulnerability being actively exploited in the wild in April 2019.

SYSTEM AFFECTED:

- All versions of Oracle WebLogic with WLS9_ASYNC and WLS-WSAT components enabled

APRIL 26 - UPDATED SYSTEMS AFFECTED:

- Oracle WebLogic versions 10.3.6.0.0 and 12.1.3.0.0

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:

A vulnerability has been discovered in Oracle WebLogic that could allow for remote code execution. This vulnerability exists within the WLS9_ASYNC and WLS-WSAT components of WebLogic, which can allow for deserialization of malicious code. An unauthenticated attacker can exploit this issue by sending crafted requests to the affected application. Successful exploitation of this vulnerability could allow for remote code execution with elevated privileges.

April 29 - UPDATED TECHNICAL SUMMARY

Oracle WebLogic has made patches available which mitigate CVE-2019-2725.

RECOMMENDATIONS:

We recommend the following actions be taken:

- As a temporary workaround, consider disabling the WLS9_ASYNC and WLS-WSAT components until a patch is available.
- When available, apply appropriate updates provided by Oracle to affected systems immediately after appropriate testing.
- Apply the Principle of Least Privilege to all systems and services.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Monitor intrusion detection systems for any signs of anomalous activity.
- Unless required, limit external network access to affected products.

APRIL 26 – UPDATED RECOMMENDATIONS:

- Apply appropriate updates provided by Oracle to affected systems immediately, after appropriate testing.

REFERENCES:

ZDNet:

<https://www.zdnet.com/article/new-oracle-weblogic-zero-day-discovered-in-the-wild/>

April 26 – UPDATED REFERENCES:

<https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html#AppendixFMW>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2725>

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

<http://www.us-cert.gov/tlp/>

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov



DISCLAIMER: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited