

*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**

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**

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

**DATE(S) ISSUED:**

09/26/2016

**SUBJECT:**

A Vulnerability in IBM WebSphere Application Server Could Allow for Remote Code Execution

**OVERVIEW:**

A vulnerability has been discovered in IBM WebSphere Application Server that can result in remote code execution. IBM WebSphere Application Server is a software framework that hosts Java based web applications. Successful exploitation could allow an unauthenticated user to take control of the affected system and perform unauthorized actions.

**THREAT INTELLIGENCE:**

There are currently no reports of this vulnerability being exploited in the wild.

**SYSTEMS AFFECTED:**

This vulnerability affects the following versions and releases of IBM WebSphere Application Server:

- Liberty
- Version 7.0.0.41 and prior
- Version 8.0.0.12 and prior
- Version 8.5.5.10 and prior
- Version 9.0.0.1 and prior

**RISK:**

**Government:**

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

**Businesses:**

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

**Home users: N/A**

**TECHNICAL SUMMARY:**

IBM WebSphere is prone to a remote code execution vulnerability. This vulnerability could allow remote attackers to execute Java code with a serialized object from untrusted sources. Attackers can exploit this issue to execute remote code on the host operating system with the privileges of root. Successful

exploitation could allow an unauthenticated user to take control of the affected system and perform unauthorized actions.

**RECOMMENDATIONS:**

The following actions should be taken:

- Install updates once released by IBM after appropriate testing.
- Apply interim fix PI62375 to vulnerable version of software until a patch is released by IBM. Installation instructions can be found at the following URL: <http://www-01.ibm.com/support/docview.wss?uid=swg24042712>
- 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.

**REFERENCES:**

**IBM:**

<http://www-01.ibm.com/support/docview.wss?uid=swg21990060>

<http://www-01.ibm.com/support/docview.wss?uid=swg24042712>

**CVE:**

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5983>

**TLP: WHITE**

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**

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