

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.

DATE(S) ISSUED:

09/23/2013

SUBJECT:

Vulnerability in Apache Struts Could Allow Remote Code Execution

OVERVIEW:

A vulnerability has been discovered in Apache Struts which could allow an attacker to take control of the affected system. Apache Struts is an open source, MVC framework used for building Java web applications. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges of the user running the application. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

Currently, there are no known working exploits and Apache has released an update that resolves this issue.

SYSTEMS AFFECTED:

- Versions 2.0.0 – 2.3.15.1 are vulnerable

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: **N/A**

DESCRIPTION:

Apache has reported that there is a vulnerability for Struts versions 2.0.0 – 2.3.15.1 that could allow for remote code execution. This vulnerability is present because the Dynamic Method Invocation within the Struts framework is enabled by default. Apache has confirmed that the Dynamic Method Invocation is known to impose possible multiple security risks but has provided no further technical details.

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an

attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Currently, there are no known working exploits and Apache has released an update that resolves this issue.

RECOMMENDATIONS:

The following actions should be taken:

- After appropriate testing, upgrade Apache Struts software to version 2.3.15.2. If upgrading is not possible, disabling the Dynamic Method Invocation can resolve this issue. In version 2.3.15.2 Dynamic Method Invocation is set to false by default.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to download or open files from un-trusted websites, unknown users, or suspicious emails.
- Remind users not to click links from unknown sources, or to click links without verifying the intended destination.

REFERENCES:

Apache:

<http://struts.apache.org/>

<http://struts.apache.org/release/2.3.x/docs/s2-019.html>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4316>

SecurityFocus:

<http://www.securityfocus.com/bid/62587>