

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:

04/25/2014

SUBJECT:

Vulnerability in Apache Struts Could Allow Remote Code Execution

EXECUTIVE SUMMARY:

A vulnerability has been discovered for Apache Software Foundation Struts versions 2.0.0 - 2.3.16.1. Apache Struts is an open source framework used for building Java web applications. Successful exploitation of this vulnerability could allow for remote code execution. 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.

THREAT INTELLIGENCE

At this time, a proof-of-concept is available outlining how to bypass a previous released patch for the latest Apache Struts version 2.3.16.1, and exploit the vulnerability.

SYSTEM AFFECTED:

- Apache Struts 2.0.0 - 2.3.16.1

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

TECHNICAL SUMMARY:

A vulnerability has been discovered in Apache Struts versions 2.0.0 - 2.3.16.1 that, when exploited, will first result in a Denial of Service (DoS) condition to bypass a previously released patch issued in version 2.3.16.1. After bypassing the patch, remote code execution becomes possible by allowing for the mapping of shared hosting directories on affected products using impacted versions of Struts. 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. The vulnerability is caused when ClassLoader manipulation exploitation occurs because of Struts failure to restrict access to the 'class' parameter which is directly mapped to 'getClass()' method through 'ParametersInterceptor'. This issue was previously thought to have been resolved by updating to version 2.3.16.1, but the patch did not resolve the issue and as a result can be bypassed and exploited.

At this time there is a proof-of-concept showing how to bypass the previous released patch and exploit the latest Struts version 2.3.16.1. Currently, Apache is working on security fix to address the vulnerability, which they expect to be available within 72 hours.

Until the security fix becomes available, mitigation steps have been made available by Apache and can be found at [hxxp://struts.apache.org/announce.html#a20140424](http://struts.apache.org/announce.html#a20140424).

RECOMMENDATIONS:

The following actions should be taken:

- Incorporate the mitigation steps found at [hxxp://struts.apache.org/announce.html#a20140424](http://struts.apache.org/announce.html#a20140424).
- Apply the update from Apache, as soon as one becomes available, after appropriate testing.

REFERENCES:

Apache:

http://mail-archives.us.apache.org/mod_mbox/www-announce/201404.mbox/%3C53592D88.8040200@apache.org%3E

<http://struts.apache.org/announce.html#a20140424>

Security Focus:

<http://www.securityfocus.com/bid/65999>

<http://www.securityfocus.com/bid/67064>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0094>

PwnTesting:

<http://www.pwntester.com/blog/2014/04/24/struts2-0day-in-the-wild/>

Nanjing Hanhai source (bypass PoC):

http://blog.vulnhunt.com/index.php/2014/04/24/apache_struts2_0day/