

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:

12/15/2015

SUBJECT:

Vulnerability in Apache Commons Collections Could Allow Arbitrary Code Execution

OVERVIEW:

A vulnerability has been discovered in Apache Commons Collections which could allow for remote code execution. Apache Commons Collections are a set of implementations, interfaces, and utilities to expand on the functionality of the Java Development Kit (JDK) classes. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the application account and allow for the execution of arbitrary code.

THREAT INTELLIGENCE

There are currently no reports of this vulnerability being exploited in the wild. There are known proof-of-concept exploits for this vulnerability.

SYSTEMS AFFECTED:

The following vendors have been found to have products affected by this vulnerability:

- Cisco: <http://msisac.cisecurity.org/advisories/2015/2015-149.cfm>
- Apache TomEE: <http://www.zerodayinitiative.com/advisories/ZDI-15-638/>

(Note: MS-ISAC will continue to update the list of affected products as more information becomes available.)

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: High

TECHNICAL SUMMARY:

A vulnerability has been discovered in the Apache Commons Collections' InvokeTransformer class that when used together with an endpoint that accepts serializable objects can cause remote code execution. This vulnerability could be exploited by de-serializing a specially crafted Java object to execute a payload of arbitrary code on the affected system.

Successful exploitation could result in an attacker gaining the same privileges as the process on the system. Depending on the privileges associated with the process, an attacker could perform actions

such as install programs; view, change, or delete data; or create new accounts with full user rights, dependent on the vulnerable application.

RECOMMENDATIONS:

The following actions should be taken:

- Apply vendor-specific updates once they become available after appropriate testing.
- Verify no unauthorized system modifications have occurred on the system before applying patches.
- Monitor intrusion detection systems for any signs of anomalous activity.

REFERENCES:

Cisco:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151209-java-deserialization>

Apache:

<https://issues.apache.org/jira/browse/COLLECTIONS-580>

foxglovesecurity:

<http://foxglovesecurity.com/2015/11/06/what-do-weblogic-websphere-jboss-jenkins-opennms-and-your-application-have-in-common-this-vulnerability/>

ZDNet:

<http://www.zdnet.com/article/java-unserialize-remote-code-execution-hole-hits-commons-collections-jboss-websphere-weblogic/>

Infoq:

<http://www.infoq.com/news/2015/11/commons-exploit>

TLP: WHITE

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

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