

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 Cisco Products Could Allow Remote Code Execution

**OVERVIEW:**

A vulnerability has been discovered affecting Cisco products. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

**THREAT INTELLIGENCE:**

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

**SYSTEMS AFFECTED:**

Products from the following Cisco product categories are affected:

- Cable Modems
- Collaboration and Social Media
- Endpoint Clients and Client Software
- Network Application, Service, and Acceleration
- Network and Content Security Devices
- Network Management and Provisioning
- Routing and Switching - Enterprise and Service Provider
- Voice and Unified Communications Devices
- Video, Streaming, TelePresence, and Transcoding Devices
- Cisco Hosted Services

Please visit the link below for a detailed list of the specific affected products:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151209-java-deserialization> (Note: Additional products may be included at a later date as Cisco is currently investigating the scope of this vulnerability).

**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 remote code execution vulnerability exists in several Cisco products due to a Java deserialization issue that is used by the Apache Commons Collections (ACC) library. An attacker may exploit this

vulnerability by submitting specially crafted input to an application on a targeted Cisco system that uses the ACC library. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

**RECOMMENDATIONS:**

The following actions should be taken:

- Verify no unauthorized system modifications have occurred on system before applying patch.
- Once a patch is released by Cisco, update immediately after appropriate testing.
- Monitor intrusion detection systems for any signs of anomalous activity.
- Unless required, limit external network access to affected products.

**REFERENCES:**

**Cisco:**

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

**CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6420>

**TLP: WHITE**

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

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