

*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:**

07/14/2015

**SUBJECT:**

Vulnerability in Adobe Shockwave Player Could Allow for Arbitrary Code Execution (APSB15-17).

**OVERVIEW:**

A vulnerability has been discovered in Adobe Shockwave that could allow an attacker to remotely take control of the affected system. Adobe Shockwave is a multimedia platform used to add animation and interactivity to web pages. Successful exploitation 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. Failed exploit attempts will likely cause denial-of-service conditions.

**THREAT INTELLIGENCE:**

There are currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEM AFFECTED:**

- Adobe Shockwave Player 12.1.8.158 and earlier for Windows and Macintosh

**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:**

Adobe has released a security update for Adobe Shockwave Player 12.1.8.158 and earlier versions on the Windows and Macintosh operating systems. This update addresses a critical memory corruption vulnerability that could potentially allow an attacker to remotely take control of the affected system. An attacker could exploit this vulnerability by creating a web site that contains specially crafted content designed to exploit this vulnerability. (CVE-2015-5120, CVE-2015-5121)

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. A failed attack can still cause a denial of service attack by causing the affected program to crash.

## **RECOMMENDATIONS:**

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

## **REFERENCES:**

### **Adobe:**

<https://helpx.adobe.com/security/products/shockwave/apsb15-17.html>

### **CVE:**

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5120>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5121>

## **TLP: WHITE**

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

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