

*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:**

02/05/2015

**SUBJECT:**

Multiple Vulnerabilities In Adobe Flash Player Could Allow Remote Code Execution (APSB15-04)

**OVERVIEW:**

Multiple vulnerabilities in Adobe Flash Player could allow remote code execution. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. Successful exploitation could result in an attacker compromising data security, potentially allowing access to confidential data, or could compromise processing resources in a user's computer. Failed exploit attempts will likely cause denial-of-service conditions.

**THREAT INTELLIGENCE**

Trend Micro has reported that CVE-2015-0313 is currently being observed in the wild in malvertising campaigns. There are currently no reports of the other vulnerabilities being exploited in the wild.

**SYSTEM AFFECTED:**

- Adobe Flash Player 16.0.0.296 and earlier versions
- Adobe Flash Player 13.0.0.264 and earlier 13.x versions
- Adobe Flash Player 11.2.202.440 and earlier 11.x versions

**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 Flash Player is prone to multiple vulnerabilities that could allow for remote code execution. These vulnerabilities are as follows:

- Use-after-free vulnerability that could lead to code execution (CVE-2015-0313, CVE-2015-0315, CVE-2015-0320, CVE-2015-0322).
- Memory corruption vulnerabilities that could lead to code execution (CVE-2015-0314, CVE-2015-0316, CVE-2015-0318, CVE-2015-0321, CVE-2015-0329, CVE-2015-0330).
- Type confusion vulnerability that could lead to code execution (CVE-2015-0317, CVE-2015-0319).
- Heap Buffer overflow vulnerabilities that could lead to code execution (CVE-2015-0323, CVE-2015-032).
- Buffer overflow vulnerability that could lead to code execution (CVE-2015-0324).

- A Null pointer dereferencing issue (CVE-2015-0325, CVE-2015-0326, CVE-2015-0328).

Successful exploitation could result in an attacker compromising data security, potentially allowing access to confidential data, or could compromise processing resources in a user's computer.

**RECOMMENDATIONS:**

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.
- Limit user account privileges to those required only.

**REFERENCES:**

**Adobe:**

<http://helpx.adobe.com/security/products/flash-player/apsb15-04.html>

**CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0313>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0314>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0315>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0316>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0317>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0318>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0319>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0320>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0321>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0322>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0323>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0324>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0325>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0326>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0327>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0328>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0329>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0330>

**SecurityFocus:**

<http://www.securityfocus.com/bid/72429>

<http://www.securityfocus.com/bid/72514>

**TLP: WHITE**

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

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