

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:

06/23/2015

SUBJECT:

Vulnerability in Adobe Flash Player Could Allow Remote Code Execution (APSB15-14)

OVERVIEW:

A vulnerability has been discovered in Adobe Flash Player, which 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 of this vulnerability could result in an attacker compromising data security, potentially allowing access to confidential data, or allow for complete control of the affected system.

THREAT INTELLIGENCE

There are reports of this vulnerability being exploited in the wild.

SYSTEM AFFECTED:

- Adobe Flash Player for Google Chrome prior to version 18.0.0.194
- Adobe Flash Player for Internet Explorer 10 and 11 prior to version 18.0.0.194
- Adobe Flash Player for Linux prior to version 11.2.202.468
- Adobe Flash Player Extended Support Release prior to version 13.0.0.296
- Adobe Desktop Runtime prior to version 18.0.0.194 for Macintosh and Windows

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 a heap buffer overflow vulnerability. Adobe has released security updates for Adobe Flash Player for Windows, Macintosh and Linux after reports of active exploits targeting systems running Internet Explorer and Firefox.

Successful exploitation of this vulnerability could result in an attacker compromising data security, potentially allowing access to confidential data, or allow for complete control of the affected system.

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 those from un-trusted sources.

REFERENCES:

Adobe:

<https://helpx.adobe.com/security/products/flash-player/apsb15-14.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3113>

TLP: WHITE

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

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