

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:

06/14/2016

SUBJECT:

A Vulnerability in Adobe Flash Player Could Allow for Remote Code Execution (APSB16-03)

OVERVIEW:

A vulnerability has been discovered in Adobe Flash Player that could allow for 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 vulnerabilities may cause a crash and allow an attacker to take control of the affected system

THREAT INTELLIGENCE:

Adobe is aware of reports that CVE-2016-4171 exists in the wild, and is being used in limited, targeted attacks. Kaspersky and Microsoft EMET mitigate the attacks. An update that addresses this patch will be made available as early as June 16.

SYSTEMS AFFECTED:

- Adobe Flash Player 21.0.0.242 and earlier versions for Windows, Macintosh, and Linux, and Chrome OS.

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: LOW

TECHNICAL SUMMARY:

Adobe Flash Player is prone to a vulnerability which could allow for remote code execution or denial of service conditions. Few details are currently available, more information should become available after Adobe releases the security update addressing this vulnerability as early as June 16.

RECOMMENDATIONS:

The following actions should be taken:

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

REFERENCES:

Adobe:

<https://helpx.adobe.com/security/products/flash-player/apsa16-03.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4171>

Kaspersky:

<https://securelist.com/blog/75082/cve-2016-4171-adobe-flash-zero-day-used-in-targeted-attacks/>

TLP: WHITE

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

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