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:
02/02/2015
02/05/2015 - Updated

SUBJECT:
Vulnerability In Adobe Flash Player Could Allow Remote Code Execution

OVERVIEW:
A zero-day 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 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. CIS will continue to monitor this vulnerability and update accordingly.

February 5 - UPDATED OVERVIEW:
Adobe Flash Player 16.0.0.305 is now available for download via auto-update as well as manually from Adobe. This version mitigates the zero-day reported previously (CVE-2015-0313). Adobe is working with their distribution partners to make the update available in Google Chrome and Internet Explorer 10 and 11.

THREAT INTELLIGENCE
This exploit has been confirmed to be in use in the wild as part of malvertising attacks and appears to be part of the Angler Exploit Kit.

SYSTEMS AFFECTED:
- Adobe Flash Player 16.0.0.296 and earlier versions for Windows and Macintosh
- Adobe Flash Player 13.0.0.264 and earlier 13.x versions
- Adobe Flash Player 11.2.202.440 and earlier versions for Linux

February 5 – UPDATED SYSTEMS AFFECTED:
- ***Adobe Flash Player 16.0.0.296 and earlier versions for Windows and Macintosh***
- ***Adobe Flash Player 13.0.0.264 and earlier 13.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:

An Adobe Flash Player zero-day vulnerability has been discovered by Trend Micro, which could allow for remote code execution. Adobe has acknowledged this vulnerability and plans to release a patch during the week.

Trend Micro reports that this vulnerability is being observed in the wild in malvertising attacks. One affected domain, dailymotion[.]com, is a popular video sharing site which, after a series of redirects, takes the user to www.retilio[.]com/skillt.swf. Due to the similarities in obfuscation techniques and infection chains, it is believed that this vulnerability is included in the Angler Exploit Kit.

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.

February 5 - UPDATED TECHNICAL SUMMARY:
Adobe Flash Player 16.0.0.305 has been made available through auto-update and manual download. This version mitigates CVE-2015-0313, which was being used in malvertising attacks.

RECOMMENDATIONS:
The following actions should be taken:

- Patch to the latest version once released and after appropriate testing.
- Consider blocking the domains reported by Trend Micro.
- 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:
Abode:
https://helpx.adobe.com/security/products/flash-player/apsa15-02.html

Trend Micro:
http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-discovers-new-adobe-flash-zero-day-exploit-used-in-malvertisements/

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0313

SecurityFocus:
http://www.securityfocus.com/bid/72429

February 5 - UPDATED REFERENCES:
http://helpx.adobe.com/security/products/flash-player/apsb15-04.html

TLP: WHITE
Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.
http://www.us-cert.gov/tlp/