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:
3/12/2015

SUBJECT:
Multiple Vulnerabilities in Adobe Flash Player Could Allow Remote Code Execution (APSB15-05)

OVERVIEW:
Multiple vulnerabilities have been discovered in Adobe Flash Player. 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
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:
- Adobe Flash Player 16.0.0.305 and earlier versions
- Adobe Flash Player 13.0.0.269 and earlier 13.x versions
- Adobe Flash Player 13.0.0.269 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:
Adobe Flash Player is prone to multiple vulnerabilities that could allow for remote code execution. These vulnerabilities are as follows:

- Memory corruption vulnerabilities that may lead to code execution (CVE-2015-0332, CVE-2015-0333, CVE-2015-0335, CVE-2015-0339).
- Type confusion vulnerabilities that may lead to code execution (CVE-2015-0334, CVE-2015-0336).
- A vulnerability that could lead to a cross-domain policy bypass (CVE-2015-0337).
- A vulnerability that may lead to a file upload restriction bypass (CVE-2015-0340).
- An integer overflow vulnerability that could lead to code execution (CVE-2015-0338).

- Use-after-free vulnerabilities that could lead to code execution (CVE-2015-0341, CVE-2015-0342).

Successful exploitation of these vulnerabilities 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 access.

RECOMMENDATIONS:
The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Remind users not to visit untrusted 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:
https://helpx.adobe.com/security/products/flash-player/apsb15-05.html

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0332
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0333
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0334
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0335
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0336
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0337
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0338
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0339
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0340
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0341
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0342

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