

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:

05/12/2015

05/27/2015 - Updated

SUBJECT:

Multiple Vulnerabilities in Adobe Flash Player Could Allow Remote Code Execution (APSB15-09)

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

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

May 27 - UPDATED THREAT INTELLIGENCE:

FireEye has confirmed that vulnerability CVE-2015-3090 has been included in the Angler Exploit Kit and is actively being exploited in the wild. Using this vulnerability, Angler Exploit Kit can compromise victim machines in order to deliver malware.

SYSTEM AFFECTED:

- Adobe Flash Player 17.0.0.169 and earlier versions
- Adobe Flash Player 13.0.0.281 and earlier 13.x versions
- Adobe Flash Player 11.2.202.457 and earlier 11.x versions
- AIR Desktop Runtime 17.0.0.144 and earlier versions
- AIR SDK and SDK & Compiler 17.0.0.144 and earlier 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. These vulnerabilities are as follows:

- Multiple memory corruption vulnerabilities that could lead to remote code execution (CVE-2015-3078, CVE-2015-3089, CVE-2015-3090, CVE-2015-3093).
- Heap overflow vulnerability that could lead to remote code execution (CVE-2015-3088).
- Time-of-check time-of-use (TOCTOU) race condition that could be exploited to bypass Protected Mode in Internet Explorer (CVE-2015-3081).
- Integer overflow vulnerability that could lead to remote code execution (CVE-2015-3087).
- Type confusion vulnerabilities that could lead to remote code execution (CVE-2015-3077, CVE-2015-3084, CVE-2015-3086).
- Use-after-free vulnerability that could lead to remote code execution (CVE-2015-3080).
- Memory leak vulnerabilities that could be used to bypass Address Space Layout Randomization (ASLR) (CVE-2015-3091, CVE-2015-3092).
- Security bypass vulnerabilities that could be exploited to write arbitrary data to the file system under user permissions (CVE-2015-3082, CVE-2015-3083, CVE-2015-3085).
- Security bypass vulnerability that could lead to information disclosure (CVE-2015-3079), and provide additional hardening to protect against CVE-2015-3044.

Successful exploitation of these vulnerabilities could result in the attacker gaining the same rights 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 rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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/apsb15-09.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3044>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3077>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3078>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3079>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3080>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3081>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3082>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3083>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3084>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3085>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3086>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3087>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3088>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3089>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3090>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3091>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3092>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3093>

May 27 – UPDATED REFERENCES:

FireEye:

https://www.fireeye.com/blog/threat-research/2015/05/angler_ek_exploiting.html

TLP: WHITE

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

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