**TLP: WHITE**
**MS-ISAC/CIS CYBER SECURITY ADVISORY**

**MS-ISAC/CIS ADVISORY NUMBER:**
2015-075

**DATE(S) ISSUED:**
07/08/2015

**SUBJECT:**
Multiple Vulnerabilities in Adobe Flash Player Could Allow Remote Code Execution (APSB15-16)

**OVERVIEW:**
Multiple vulnerabilities have been discovered in Adobe Flash Player, 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**
Proof of concept code is publicly available for CVE-2015-5119, a use-after-free vulnerability that could lead to remote code execution. There are reports of this vulnerability being exploited in the wild, specifically by the Angler Exploit Kit and Nuclear Exploit Pack.

**SYSTEM AFFECTED:**

- Adobe Flash Player prior to version 18.0.0.203
- Adobe Flash Player Extended Support Release prior to version 13.0.0.302
- Adobe Flash Player for Linux prior to version 11.2.202.481
- Adobe Flash Player for Google Chrome prior to version 18.0.0.203 for Windows and Macintosh
- Adobe Flash Player for Google Chrome prior to version 18.0.0.204 for Linux
- Adobe Flash Player for Internet Explorer 10 and 11 prior to version 18.0.0.203
- Adobe AIR Desktop Runtime prior to version 18.0.0.180 for Macintosh
- Adobe AIR SDK and SDK & Compiler prior to version 18.0.0.80

**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:

- Heap buffer overflow vulnerability that could lead to code execution (CVE-2015-3135, CVE-2015-4432, CVE-2015-5118)
- Memory corruption vulnerability that could lead to code execution (CVE-2015-3117, CVE-2015-3123, CVE-2015-3130, CVE-2015-3133, CVE-2015-3134, CVE-2015-4431)
- Type confusion vulnerability that could lead to code execution (CVE-2015-3119, CVE-2015-3120, CVE-2015-3121, CVE-2015-3122, CVE-2015-4433)
- Use-after-free vulnerabilities that could lead to code execution (CVE-2015-3118, CVE-2015-3124, CVE-2015-5117, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, CVE-2015-5119) **Updates MS-ISAC Advisory 2015-074**
- Security bypass vulnerability that could lead to information disclosure (CVE-2015-3114)
- Multiple vulnerabilities that could be exploited to bypass the same-origin-policy and lead to information disclosure (CVE-2014-0578, CVE-2015-3115, CVE-2015-3116, CVE-2015-3125, CVE-2015-5116)
- These updates improve memory address randomization of Flash heap for Windows 7 64-bit (CVE-2015-3097)
- These updates resolve null pointer dereference issues (CVE-2015-3126, CVE-2015-4429)

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.

**RECOMMENDATIONS:**
We recommend the following actions 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/apsb15-16.html

**CVE:**
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0578
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3097
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3114
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3115
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3116
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3117
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3118
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3119
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3120
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3121
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3122
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3123
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3124
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3125
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3126
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3127
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3128
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3129
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3130
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3131
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3132
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3133
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3134

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3135
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3136
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3137
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4428
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4429
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4430
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4431
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4432
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4433
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5117
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5118
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5119

**Trend Micro:**
http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-flash-zero-day-integrated-into-exploit-kits/