



**State of Alaska Cyber Security &  
Critical Infrastructure  
Cyber Advisory**

**June 14, 2016**

*The following cyber advisory was issued by the State of Alaska and was 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.*

**ADVISORY NUMBER:**

SA2016-095

**DATE(S) ISSUED:**

06/14/2016

**06/16/2016 - UPDATED**

**SUBJECT:**

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

***June 16 – UPDATED SUBJECT:***

***Multiple Vulnerabilities in Adobe Flash Player Could Allow for Remote Code Execution (APSB16-18)***

**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.

***June 16 – UPDATED OVERVIEW:***

***Multiple vulnerabilities have been discovered in Adobe Flash Player, the most severe of which could allow for remote code execution. Successful exploitation of these 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.

**June 16 – UPDATED 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. CVE-2016-4132 has been publicly disclosed by Cisco's Talos.***

**SYSTEMS AFFECTED:**

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

**June 16 – UPDATED SYSTEMS AFFECTS:**

- ***Adobe Flash Player versions prior to 22.0.0.192 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.

**June 16 - TECHNICAL SUMMARY:**

***Multiple vulnerabilities have been discovered in Adobe Flash Player the most severe of which could allow for remote code execution. These vulnerabilities are as follows:***

- ***These updates resolve type confusion vulnerabilities that could lead to code execution (CVE-2016-4144, CVE-2016-4149).***
- ***These updates resolve use-after-free vulnerabilities that could lead to code execution (CVE-2016-4142, CVE-2016-4143, CVE-2016-4145, CVE-2016-4146, CVE-2016-4147, CVE-2016-4148).***
- ***These updates resolve heap buffer overflow vulnerabilities that could lead to code execution (CVE-2016-4135, CVE-2016-4136, CVE-2016-4138).***
- ***These updates resolve memory corruption vulnerabilities that could lead to code execution (CVE-2016-4122, CVE-2016-4123, CVE-2016-4124, CVE-2016-***

**4125, CVE-2016-4127, CVE-2016-4128, CVE-2016-4129, CVE-2016-4130, CVE-2016-4131, CVE-2016-4132, CVE-2016-4133, CVE-2016-4134, CVE-2016-4137, CVE-2016-4141, CVE-2016-4150, CVE-2016-4151, CVE-2016-4152, CVE-2016-4153, CVE-2016-4154, CVE-2016-4155, CVE-2016-4156, CVE-2016-4166, CVE-2016-4171).**

- ***These updates resolve a vulnerability in the directory search path used to find resources that could lead to code execution (CVE-2016-4140).***
- ***These updates resolve a vulnerability that could be exploited to bypass the same-origin-policy and lead to information disclosure (CVE-2016-4139).***

***Successful exploitation of these vulnerabilities may allow for remote code execution in the context of the current user. Failed exploit attempts will likely result in denial of service conditions.***

#### **RECOMMENDATIONS:**

We recommend the following actions be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Consider disabling Adobe Flash Player until the patch is applied.
- 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/>

#### **June 16 – REFERENCES:**

**Adobe:**

<https://helpx.adobe.com/security/products/flash-player/apsb16-18.html>

**Talos:**

<http://www.talosintel.com/reports/TALOS-2016-0165/>