



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

January 23, 2015

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:

SA2015-004A - **UPDATED**

DATE(S) ISSUED:

01/22/2015

01/23/2015 - Updated

SUBJECT: A vulnerability In Adobe Flash Player Could Allow Remote Code Execution (APSB15-02)

OVERVIEW:

A vulnerability in Adobe Flash Player 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.

January 23 - UPDATED OVERVIEW:

Two additional vulnerabilities have been reported in Adobe Flash Player which could allow for remote code execution.

THREAT INTELLIGENCE:

This exploit has been confirmed to be included in the Angler Exploit Kit and is actively being used in the wild. Adobe is investigating reports that a separate exploit for Flash Player 16.0.0.287 and earlier versions also exists in the wild. CIS is monitoring this claim and will update this advisory as information becomes available.

January 23 - UPDATED THREAT INTELLIGENCE:

These exploits have been confirmed to be included in the Angler Exploit Kit and are actively being used in the wild. Adobe has confirmed the existence of the Zero Day affecting Adobe Flash Player 16.0.0.287 and has assigned CVE-2015-0311 to it. Adobe expects to have a patch available for CVE-2015-0311 during the week of January 26. CIS will update this advisory when the new patch becomes available. Please note that while Adobe Flash Player 16.0.0.287 is still vulnerable it does mitigate CVE-2015-0310.

SYSTEM AFFECTED:

- Adobe Flash Player 16.0.0.257 and earlier versions
- Adobe Flash Player 13.0.0.260 and earlier 13.x versions
- Adobe Flash Player 11.2.202.429 and earlier versions for Linux

January 23 - UPDATED SYSTEM AFFECTED:

- ***Adobe Flash Player 16.0.0.287 and earlier versions for Windows and Macintosh***
- ***Adobe Flash Player 13.0.0.262 and earlier 13.x versions***
- ***Adobe Flash Player 11.2.202.438 and earlier versions for Linux***

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 a vulnerability that could allow a remote attacker to circumvent the memory randomization mitigations on the Windows platform.

This could give the attacker the ability to run remote code on the system with the same permissions level as the user/browser has.

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.

The following registry keys can be used to prevent Adobe Flash Player from being initiated by Internet Explorer or Microsoft Office Products by pasting the following into a text file with the .reg extension and then running the file.

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX  
Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}]
```

```
"Compatibility Flags"=dword:00000400
```

```
[HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\Microsoft\Internet  
Explorer\ActiveX Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}]
```

```
"Compatibility Flags"=dword:00000400
```

To remove this workaround delete the registry keys that were created above.

Of note this advisory covers CVE-2015-0310 which was successfully mitigated in Adobe Flash Player 16.0.0.287. This does not encompass the zero day being reported by the media, which Adobe is still in the process of validating and mitigating.

January 23 - UPDATED TECHNICAL SUMMARY:

Adobe Flash Player is prone to two vulnerabilities that could allow a remote attacker to circumvent the memory randomization mitigations on the Windows platform. This could give the attacker the ability to run remote code on the system with the same permissions level as the user/browser has. 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.

Of note Adobe Flash Player 16.0.0.287 only mitigates CVE-2015-0310, and does not protect against CVE-2015-0311. Adobe expects to have a patch available for CVE-2015-0311 during the week of January 26.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Utilize Google Chrome for web browsing as it may not be vulnerable to this exploit.
- Do not open email attachments from unknown or untrusted sources.
- Limit user account privileges to those required only.

REFERENCES:

Symantec:

<http://www.symantec.com/connect/blogs/unconfirmed-zero-day-vulnerability-discovered-adobe-flash-player>

Trend Micro:

<http://blog.trendmicro.com/trendlabs-security-intelligence/flash-greets-2015-with-new-zero-day/>

Microsoft:

<https://technet.microsoft.com/library/security/2755801>

Adobe:

<http://helpx.adobe.com/security/products/flash-player/apsb15-02.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0310>

Security Focus:

<http://www.securityfocus.com/bid/72261>

January 23 - UPDATED REFERENCES:

Adobe:

<http://helpx.adobe.com/security/products/flash-player/apsa15-01.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-03110>

SecurityFocus:

<http://www.securityfocus.com/bid/72283>