



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

**February 7, 2013**

*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:**  
SA2013-010

**DATE(S) ISSUED:**  
02/07/2013

**SUBJECT:**  
Multiple Vulnerabilities in Adobe Flash Player Could Allow For Remote Code Execution  
(APSB13-04)

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Adobe Flash Player that could allow an attacker to take control of the affected system. 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 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 rights. Failed exploit attempts will likely cause denial-of-service conditions.

**It should be noted that these vulnerabilities are currently being exploited via various phishing campaigns.**

**SYSTEMS AFFECTED:**

- Adobe Flash Player 11.5.502.146 and earlier versions for Windows and Macintosh
- Adobe Flash Player 11.2.202.261 and earlier versions for Linux
- Adobe Flash Player 11.1.115.36 and earlier versions for Android 4.x
- Adobe Flash Player 11.1.111.31 and earlier versions for Android 3.x and 2.x

**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**

**DESCRIPTION:**

Adobe Flash Player is prone to multiple vulnerabilities that could allow for remote code execution. Adobe has released security updates for Adobe Flash Player 11.5.502.146 and earlier versions for Windows and Macintosh, Adobe Flash Player 11.2.202.261 and earlier versions for Linux, Adobe Flash Player 11.1.115.36 and earlier versions for Android 4.x, and Adobe Flash Player 11.1.111.31 and earlier versions for Android 3.x and 2.x.

Successful exploitation 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 rights. Failed exploit attempts will likely cause denial-of-service conditions.

***CVE-2013-0633* - This vulnerability is being exploited in the wild in targeted attacks designed to trick the users into opening a Microsoft Word document delivered as an email attachment which contains malicious Flash (SWF) content. The exploit targets the ActiveX version of Flash Player on Windows.**

***CVE-2013-0634* - This vulnerability is being exploited in the wild in attacks delivered via malicious Flash (SWF) content hosted on websites that target Flash Player in Firefox or Safari on the Macintosh platform, as well as attacks designed to trick Windows users into opening a Microsoft Word document delivered as an email attachment which contains malicious Flash (SWF) content.**

#### **RECOMMENDATIONS:**

We recommend the following actions be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Users of Adobe Flash Player 11.5.502.146 and earlier versions for Windows and Macintosh should update to Adobe Flash Player 11.5.502.149.
- Users of Adobe Flash Player 11.2.202.261 and earlier versions for Linux should update to Adobe Flash Player 11.2.202.262.
- Users of Adobe Flash Player 11.1.115.36 and earlier versions on Android 4.x devices should update to Adobe Flash Player 11.1.115.37.
- Users of Adobe Flash Player 11.1.111.31 and earlier versions for Android 3.x and earlier versions should update to Flash Player 11.1.111.32.
- 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 untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.

## **REFERENCES:**

### **Adobe:**

<http://www.adobe.com/support/security/bulletins/apsb13-04.html>

### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0633>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0634>

### **Security Focus:**

<http://www.securityfocus.com/bid/57787>

<http://www.securityfocus.com/bid/57788>