



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

**April 9, 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:**

SA2013-034

**DATE(S) ISSUED:**

04/09/2013

**SUBJECT:**

Multiple Vulnerabilities in Adobe Flash Player and Adobe AIR Could Allow Remote Code Execution (APSB13-11)

**OVERVIEW:**

Multiple security updates have been released for Adobe Flash Player and Adobe AIR. Adobe Flash Player and Adobe AIR are widely distributed multimedia and application players used to enhance the user experience when visiting web pages or reading email messages. Adobe Flash Player is prone to seventeen vulnerabilities that could allow for remote code execution or information disclosure.

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.

**SYSTEM AFFECTED:**

- Adobe Flash Player 11.6.602.180 and earlier versions for Windows and Macintosh
- Adobe Flash Player 11.2.202.275 and earlier versions for Linux
- Adobe Flash Player 11.1.115.48 and earlier versions for Android 4.x
- Adobe Flash Player 11.1.111.44 and earlier versions for Android 3.x and 2.x
- Adobe AIR 3.6.0.6090 and earlier versions for Windows, Macintosh and Android
- Adobe AIR 3.6.0.6090 SDK & Compiler 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**

**DESCRIPTION:**

Adobe Flash Player and AIR are prone to multiple vulnerabilities that could allow for remote code execution. The update provided by Adobe resolves the following:

- An integer overflow vulnerability that could lead to code execution (CVE-2013-2555).
- A memory corruption vulnerabilities that could lead to code execution (CVE-2013-1378, CVE-2013-1380).
- A memory corruption vulnerability caused by Flash Player improperly initializing certain pointer arrays, which could lead to code execution (CVE-2013-1379).
- Attackers can exploit these issues to execute arbitrary code in the context of the affected application. Failed exploit attempts will likely result in denial-of-service conditions.

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.

**RECOMMENDATIONS:**

We recommend the following actions be taken:

- Update Adobe Flash Player on vulnerable systems immediately after testing.
- Users of Adobe Flash Player 11.6.602.180 and earlier versions for Windows and Macintosh should update to Adobe Flash Player 11.7.700.169.
- Users of Adobe Flash Player 11.2.202.275 and earlier versions for Linux should update to Adobe Flash Player 11.2.202.280.
- 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 attachments and hypertext links contained in emails especially from un-trusted sources.

**REFERENCES:**

**Adobe:**

<http://www.adobe.com/support/security/bulletins/apsb13-11.html>

**Security Focus:**

<http://www.securityfocus.com/bid/58947>

<http://www.securityfocus.com/bid/58949>

<http://www.securityfocus.com/bid/58951>

<http://www.securityfocus.com/bid/58952>

**CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1378>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1379>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1380>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2555>