



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

March 26, 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:

SA2013-026

DATE(S) ISSUED:

03/12/2012

SUBJECT:

Adobe Flash Player Remote Code Execution Vulnerability (APSB13-09)

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 multimedia application for multiple platforms.

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.

SYSTEMS AFFECTED:

- Adobe Flash Player 11.6.602.171 and earlier versions for Windows and Macintosh
- Adobe Flash Player 11.2.202.273 and earlier versions for Linux
- Adobe Flash Player 11.1.115.47 and earlier versions for Android 4.x
- Adobe Flash Player 11.1.111.43 and earlier versions for Android 3.x and 2.x
- Adobe AIR 3.6.0.597 and earlier versions for Windows, Macintosh and Android
- Adobe AIR 3.6.0.597 SDK and earlier versions
- Adobe AIR 3.6.0.599 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 is 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-2013-0646).
- A use-after-free vulnerability that could be exploited to execute arbitrary code (CVE-2013-0650).
- A memory corruption vulnerability that could lead to code execution (CVE-2013-1371).
- A heap buffer overflow vulnerability that could lead to code execution (CVE-2013-1375).

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 Shockwave Player on vulnerable systems immediately after testing.
- Users of Adobe Flash Player 11.6.602.171 and earlier versions for Windows and Macintosh should update to Adobe Flash Player 11.6.602.180.
- Users of Adobe Flash Player 11.2.202.273 and earlier versions for Linux should update to Adobe Flash Player 11.2.202.275.
- 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:

<https://www.adobe.com/support/security/bulletins/apsb13-09.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0646>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0650>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1371>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1375>

Security Focus:

<http://www.securityfocus.com/bid/58396>