



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

October 14, 2014

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:

SA2014-067

DATE(S) ISSUED:

10/14/2014

SUBJECT:

Multiple vulnerabilities found in Adobe Flash Player and Adobe AIR could allow an attacker to execute code remotely. (APSB14-22)

EXECUTIVE SUMMARY:

Multiple vulnerabilities in Adobe Flash Player and Adobe AIR 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. Adobe AIR is a cross platform runtime used for developing Internet applications that run outside of a browser.

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.

THREAT INTELLIGENCE

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

- Adobe Flash Player 15.0.0.167 and earlier versions
- Adobe Flash Player 13.0.0.244 and earlier 13.x versions
- Adobe Flash Player 11.2.202.406 and earlier versions for Linux
- Adobe AIR desktop runtime 15.0.0.249 and earlier versions
- Adobe AIR SDK 15.0.0.249 and earlier versions
- Adobe AIR SDK & Compiler 15.0.0.249 and earlier versions
- Adobe AIR 15.0.0.252 and earlier versions for Android

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 multiple vulnerabilities that could allow for remote code execution. These vulnerabilities are as follows:

- Memory corruption vulnerabilities that could lead to code execution (CVE-2014-0564, CVE-2014-0558).
- Integer overflow vulnerability that could lead to code execution (CVE-2014-0569).

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.

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.
- Do not open email attachments from unknown or untrusted sources.
- Limit user account privileges to those required only.

REFERENCES:

Adobe:

<http://helpx.adobe.com/security/products/flash-player/apsb14-22.html>

Security Focus:

<http://www.securityfocus.com/bid/70437>

<http://www.securityfocus.com/bid/70441>

<http://www.securityfocus.com/bid/70442>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0558>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0564>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0569>