



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

May 13, 2011

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:

SA2011-032

DATE(S) ISSUED:

05/13/2011

05/25/2011 - UPDATED

SUBJECT:

Multiple Vulnerabilities in Adobe Flash Player Could Allow For Remote Code Execution (APSB11-12)

ORIGINAL OVERVIEW:

Multiple vulnerabilities have been discovered in Adobe Flash Player that could allow attackers to take complete control of affected systems. 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.

One of these vulnerabilities may be exploited if a user opens a Microsoft Word or Microsoft Excel document containing an embedded, specially crafted Adobe Flash file, which may be sent as an email attachment. Adobe is reporting that there is malware attempting to exploit this vulnerability.

May 24 – UPDATED OVERVIEW:

An additional integer overflow vulnerability has been identified in Adobe Flash Player that could allow attackers to remotely execute arbitrary code. It should be noted that if you have already applied the patch provided by Adobe mentioned in our original advisory, your systems are not vulnerable and you do not need to re-apply the patch.

SYSTEMS AFFECTED:

- AdobeFlash Player 10.2.159.1 and earlier versions for Windows, Macintosh, Linux and Solaris operating systems.
- AdobeFlash Player 10.2.154.28 and earlier for Chrome users.
- AdobeFlash Player 10.2.157.51 and earlier 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

DESCRIPTION:

AdobeFlash Player is prone to multiple vulnerabilities that could allow for remote code execution. Details of these vulnerabilities are as follows:

A design flaw that could lead to information disclosure;
An integer overflow vulnerability that could lead to code execution;
Five vulnerabilities involving memory corruption that could lead to code execution; and
Four bounds checking vulnerabilities that could lead to code execution.

There have been reports indicating active exploitation of one of the vulnerabilities (CVE-2011-0627) that can be exploited by opening a Microsoft Word (.doc) or Microsoft Excel(.xls) file sent as an email attachment and embedded with a specially crafted Flash (.swf) file.

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.

May 25 – UPDATED DESCRIPTION:

Adobe Flash Player is prone to a remote integer-overflow vulnerability as it fails to properly bounds check user-supplied input. This exploit may allow an attacker to execute arbitrary code in the context of the user running the affected application. Failure to exploit the vulnerability will likely result in a denial-of-service condition.

It should be noted that if you have already applied the patch provided by Adobe mentioned in our original advisory, your systems are not vulnerable and you do not need to re-apply the patch.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Install the update from Adobe immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Consider installing and running Adobe Reader X in Protected Mode.
- Do not open email attachments from unknown or untrusted sources.

- Consider implementing file extension whitelists for allowed e-mail attachments.

REFERENCES:

Adobe:

<http://www.adobe.com/support/security/bulletins/apsb11-12.html> (Updated May 25)

SecurityFocus:

<http://www.securityfocus.com/bid/46202>

<http://www.securityfocus.com/bid/47806>

<http://www.securityfocus.com/bid/47807>

<http://www.securityfocus.com/bid/47808>

<http://www.securityfocus.com/bid/47809>

<http://www.securityfocus.com/bid/47810>

<http://www.securityfocus.com/bid/47811>

<http://www.securityfocus.com/bid/47812>

<http://www.securityfocus.com/bid/47813>

<http://www.securityfocus.com/bid/47814>

<http://www.securityfocus.com/bid/47815>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0589>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0618>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0619>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0620>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0621>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0622>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0623>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0624>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0625>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0626>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0627>

UPDATED REFERENCES:

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0628>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0627>