



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

February 17, 2010

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:

SA2010-013

DATE(S) ISSUED:

2/17/2010

SUBJECT:

Multiple Vulnerabilities Discovered in Adobe Products

OVERVIEW:

Multiple vulnerabilities have been discovered in Adobe Flash Player, Adobe AIR, Adobe Reader, and Adobe Acrobat. Adobe Flash Player is a multimedia application for Microsoft Windows, Mozilla, and Apple technologies used to enhance the user experience when visiting web sites. Adobe AIR is a cross-platform runtime for developing internet applications on the desktop. Adobe Reader allows users to view Portable Document Format (PDF) files. Adobe Acrobat offers users additional features such as the ability to create PDF files. An attacker can exploit the Adobe Acrobat and Reader vulnerabilities by users opening a specially crafted PDF document. An attacker can exploit the Adobe Air and Flash Player vulnerabilities by users visiting a specially crafted website.

Successful exploitation of one of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, the attacker could then install programs; view, change, or delete data; or create new accounts with full privileges.

SYSTEMS AFFECTED:

- Adobe Flash Player 10.0.42.34 and earlier
- Adobe AIR 1.5.3.9120 and earlier
- Adobe Reader 9.3 and earlier
- Adobe Reader 8.2 and earlier
- Adobe Acrobat 9.3 and earlier
- Adobe Acrobat 8.2 and earlier

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:**

Multiple vulnerabilities have been identified in Adobe Flash Player, Adobe AIR, and Adobe Reader, which include cross-domain scripting and remote code execution. These vulnerabilities may be exploited if a user visits a specifically crafted web page, or opens a specially crafted file.

Adobe Flash Player, AIR, Adobe Reader, and Adobe Acrobat Cross Domain Scripting Vulnerability

Adobe Flash Player and AIR are prone to a cross-domain scripting vulnerability. This vulnerability arises due to an unspecified error while enforcing cross-domain requests. An attacker can exploit this vulnerability if the user visits a specially crafted web page. Successful exploitation of this vulnerability could allow an attacker to bypass the domain sandbox, perform unauthorized cross-domain requests, or launch spoofing attacks against other sites.

Adobe Reader and Adobe Acrobat Remote Code Execution Vulnerability

A remote code execution vulnerability exists in Adobe Reader. An attacker can exploit this vulnerability if a user opens a specially crafted PDF file. Successful exploitation of this vulnerability could allow for the execution arbitrary code on the affected system. 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.

Adobe Flash Player and AIR Unspecified Denial of Service Vulnerability

Adobe Flash Player and AIR are prone to a denial of service vulnerability. An attacker can exploit this vulnerability if a user opens a specially crafted flash file. This issue can be exploited to cause the affected applications to crash.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Adobe to vulnerable systems immediately after appropriate testing.
- Remind users not to visit un-trusted websites or to download or open files from un-trusted websites.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Adobe:

<http://www.adobe.com/support/security/bulletins/apsb10-06.html>

<http://www.adobe.com/support/security/bulletins/apsb10-07.html>

Security Focus:

<http://www.securityfocus.com/bid/38198>

<http://www.securityfocus.com/bid/38195>

<http://www.securityfocus.com/bid/38200>

Secunia:

<http://secunia.com/advisories/38547>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0186>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0187>