



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

April 21, 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:

SA2011-029

DATE(S) ISSUED:

4/21/2011

SUBJECT:

Vulnerability in Adobe Reader and Adobe Acrobat Could Allow For Remote Code Execution

OVERVIEW:

A vulnerability has been discovered in the Adobe Acrobat and Adobe Reader applications which could allow attackers to execute arbitrary code on the affected systems. Adobe Reader allows users to view Portable Document Format (PDF) files while Adobe Acrobat offers users additional features such as the ability to create PDF files. This vulnerability may be exploited if a user visits or is redirected to a specially crafted web page or when a user opens a specially crafted PDF 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.

This update also fixes the vulnerability identified in MS-ISAC advisory 2011-017.

SYSTEMS AFFECTED:

- Adobe Reader X (10.0.1) and earlier versions for Windows
- Adobe Reader X (10.0.2) and earlier versions for Macintosh
- Adobe Acrobat X (10.0.2) and earlier versions for Windows and Macintosh

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 Reader and Adobe Acrobat are prone to a remote code execution vulnerability when handling malicious PDF files. This vulnerability exists due to an unspecified memory corruption issue in 'cooltype.dll' when handling PDF files. The vulnerability may be exploited if a user visits or is redirected to a specially crafted web page which contains a specially crafted PDF file or when a user opens a specially crafted PDF file sent as an email attachment.

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.

This update also fixes the vulnerability identified in MS-ISAC advisory 2011-017.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Install the patch/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.
- Remind users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.

REFERENCES:**Adobe:**

<http://www.adobe.com/support/security/bulletins/apsb11-08.html>

Security Focus:

<http://www.securityfocus.com/bid/47531>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0610>