



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

**June 24, 2008**

*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.*

**STATE OF ALASKA ADVISORY NUMBER:**

2008-015

**DATE(S) ISSUED:**

June 24, 2008

**SUBJECT:**

New Vulnerability in Adobe Acrobat and Adobe Reader That May Allow Remote Code Execution

**OVERVIEW:**

A new vulnerability has been discovered in the Adobe Acrobat and Adobe Reader applications that allows attackers to execute arbitrary code on the affected systems. 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.

If successfully exploited, this vulnerability could allow an attacker to take complete control of an affected system resulting in the attacker gaining the same privileges as the logged on user. If the user is logged in with administrator privileges, the attacker could then install programs, view, change, or delete data, or create new accounts with

full privileges. Unsuccessful exploitation attempts may cause these programs to crash.

**Note: Adobe has acknowledged reports of current active exploitation of this vulnerability.**

**SYSTEMS AFFECTED:**

- Adobe Reader 8.0 through 8.12
- Adobe Reader 7.0.9 and earlier
- Adobe Acrobat Professional, 3D and Standard 8.0 through 8.1.2
- Adobe Acrobat Professional, 3D and Standard 7.0.9 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:**

Adobe has not issued any additional details regarding this vulnerability.

**RECOMMENDATIONS:**

The following actions are recommended:

- Update vulnerable Adobe software immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Update your anti-virus software signatures on all desktops, laptops and servers as soon as possible.

**REFERENCES:**

**Adobe:**

<http://www.adobe.com/support/security/bulletins/apsb08-15.html>

<http://www.adobe.com/support/downloads/detail.jsp?ftplID=3967>

**SecurityFocus:**

<http://www.securityfocus.com/bid/29908>

**CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2641>