



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

February 14, 2013

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:

SA2013-019

DATE(S) ISSUED:

2/14/2013

SUBJECT:

Multiple Vulnerabilities in Adobe Reader and Acrobat Could Allow For Remote Code Execution (APSA13-02)

OVERVIEW:

Multiple vulnerabilities have been discovered in Adobe Reader and Adobe Acrobat that could allow an attacker to take control of the affected system. 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. 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.

It should be noted that these vulnerabilities are being exploited in the wild in targeted attacks designed to trick Windows users into clicking on a malicious PDF file delivered in an email message. Adobe is in the process of working on a fix for these issues.

SYSTEMS AFFECTED:

- Adobe Reader XI (11.0.01 and earlier) for Windows and Macintosh
- Adobe Reader X (10.1.5 and earlier) for Windows and Macintosh
- Adobe Reader 9.5.3 and earlier 9.x versions for Windows, Macintosh and Linux
- Adobe Acrobat XI (11.0.01 and earlier) for Windows and Macintosh
- Adobe Acrobat X (10.1.5 and earlier) for Windows and Macintosh
- Adobe Acrobat 9.5.3 and earlier 9.x 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 Acrobat are prone to multiple vulnerabilities that could allow for remote code execution. Details of these vulnerabilities are as follows:

- Multiple unspecified vulnerabilities that could lead to code execution (CVE-2013-0640, CVE-2013-0641).

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.

It should be noted that these vulnerabilities are being exploited in the wild in targeted attacks designed to trick Windows users into clicking on a malicious PDF file delivered in an email message. Adobe is in the process of working on a fix for these issues.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Consider installing and running Adobe Reader in Protected View mode.
- 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/advisories/apsa13-02.html>

SecurityFocus:

<http://www.securityfocus.com/bid/57931>

<http://www.securityfocus.com/bid/57947>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0640>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0641>