



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

March 26, 2009

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:

SA2009-016

DATE(S) ISSUED:

03/26/2009

SUBJECT:

Vulnerabilities in Adobe Reader and Adobe Acrobat Could Allow Remote Code Execution

OVERVIEW:

New vulnerabilities have been reported in the Adobe Acrobat and Adobe Reader applications that allow attackers to execute arbitrary code on 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. Recently there have been multiple vulnerabilities and related updates announced by Adobe. The newly announced vulnerabilities in this advisory are addressed by applying the updates described in our recent advisory and associated updates (2009-008) and the related Adobe announcement.

Depending on the privileges associated with the user, an attacker could exploit these recently announced vulnerabilities to install programs; view, change, or delete data; or create new accounts with full user rights. Unsuccessful exploitation attempts may cause these programs to crash.

SYSTEMS AFFECTED:

- Adobe Reader 9 and earlier versions
- Adobe Acrobat 9 Standard, Pro, and Pro Extended and earlier versions

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 multiple remote code execution vulnerabilities. One vulnerability is a heap-based buffer-overflow vulnerability which occurs when handling JBIG2 image streams. Three other unspecified vulnerabilities allow for remote-code execution when handling JBIG2 image streams. JBIG2 is an image encoding format that is primarily used for encoding monochrome images such as faxes. An input validation vulnerability exists in a JavaScript method that could lead to remote code execution of versions 7 and 9 of the Adobe products. The update to version 7 of Adobe products also corrects three additional vulnerabilities. Testing by iDefense has shown that disabling JavaScript in Adobe Reader and Adobe Acrobat will not prevent all attacks from happening, but will make it harder for an attacker to exploit these vulnerabilities.

While these vulnerabilities are in addition to the ones that were announced in the security updates announced earlier this month, they are addressed by applying the updates referenced in the advisories we issued earlier this month. If your organization applied the updates earlier this month, no action is required.

Adobe has released updated Adobe Reader, Standard and Professional versions 7.1.1, 8.1.4, and 9.1 to fix these vulnerabilities.

RECOMMENDATIONS:

We recommend the following actions be taken:

- To mitigate this issue, those running Adobe Reader, Standard and Professional versions 7, 8, or 9 should update to versions 7.1.1, 8.1.4, or 9.1 immediately after appropriate testing.
- Consider disabling JavaScript in Adobe by navigating to Edit->Preferences and unchecking 'Enable Acrobat JavaScript'.
- Ensure antivirus software signatures are current.
- Do not open email attachments from unknown or un-trusted sources.
- Provide user awareness notification about this vulnerability and exploit.
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Adobe:

<http://www.adobe.com/support/security/bulletins/apsb09-04.html>
<http://blogs.adobe.com/psirt/>

iDefense:

<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=776>

Secunia:

http://secunia.com/secunia_research/2009-14/

Security Focus:

<http://www.securityfocus.com/archive/1/49C938EC.80005@iddefense.com>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4813>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0193>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0658>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0927>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0928>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1061>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1062>