



State of Alaska
State Security Office

Department of Administration
Enterprise Technology Services

State of Alaska Cyber Security &
Critical Infrastructure Cyber Advisory

May 14, 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.

STATE OF ALASKA ADVISORY NUMBER:

SA2009-027

DATE(S) ISSUED:

05/14/09

Subject:

Adobe Reader and Acrobat JavaScript Vulnerabilities

Source:

US-CERT / Adobe

Systems Affected:

- Adobe Reader versions 9.1, 8.1.4, 7.1.1 and earlier
- Adobe Acrobat Standard, Pro, and Pro Extended versions 9.1, 8.1.4, 7.1.1 and earlier

Overview:

Adobe has released Security Bulletin APSPB09-06, which describes Adobe Reader and Acrobat updates for two JavaScript vulnerabilities that could allow a remote attacker to execute arbitrary code.

An attacker could exploit these vulnerabilities by convincing a user to open a specially crafted Adobe Portable Document Format (PDF) file. Acrobat integrates with popular web browsers, and visiting a website is usually sufficient to cause Reader or Acrobat to open a PDF file.

Recommendations / Resolution:

Update

Adobe has released updates to address this issue. Users are encouraged to read Adobe Security Bulletin APSPB09-06 and update vulnerable versions of Adobe Reader and Acrobat. According to

APSB09-06, these vulnerabilities are addressed in versions 9.1.1, 8.1.5, and 7.1.2 of Adobe Reader and Acrobat.

Disable JavaScript in Adobe Reader and Acrobat

Disabling JavaScript prevents these vulnerabilities from being exploited and reduces attack surface. If this workaround is applied to updated versions of the Adobe Reader and Acrobat, it may protect against future vulnerabilities.

To disable JavaScript in Adobe Reader:

1. Open Adobe Acrobat Reader.
2. Open the Edit menu.
3. Choose the Preferences... option.
4. Choose the JavaScript section.
5. Uncheck the Enable Acrobat JavaScript check box.

Disabling JavaScript will not resolve the vulnerabilities; it will only disable the vulnerable JavaScript component. When JavaScript is disabled, Adobe Reader and Acrobat prompt to re-enable JavaScript when opening a PDF that contains JavaScript.

Prevent Internet Explorer from automatically opening PDF documents

The installer for Adobe Reader and Acrobat configures Internet Explorer to automatically open PDF files without any user interaction. This behavior can be reverted to the safer option of prompting the user by importing the following as a .REG file:

```
Windows Registry Editor Version 5.00
[HKEY_CLASSES_ROOT\AcroExch.Document.7]"EditFlags"=hex:00,00,00,00
```

Disable the display of PDF documents in the web browser

Preventing PDF documents from opening inside a web browser reduces attack surface. If this workaround is applied to updated versions of the Adobe Reader and Acrobat, it may protect against future vulnerabilities. To prevent PDF documents from automatically being opened in a web browser with Adobe Reader:

1. Open Adobe Acrobat Reader.
2. Open the Edit menu.
3. Choose the preferences option.
4. Choose the Internet section.
5. Un-check the "Display PDF in browser" check box.

Rename or remove Annots.api

To disable the vulnerable getAnnots() method, rename or remove the Annots.api file. This will disable some Annotation functionality, however annotations can still be viewed. This does not protect against the customDictionaryOpen() vulnerability. On Windows, Annots.api is typically located here: "%ProgramFiles%\Adobe\Reader 9.0\Reader\plug_ins"

Do not access PDF documents from untrusted sources

Do not open unfamiliar or unexpected PDF documents, particularly those hosted on web sites or delivered as email attachments. Please see Cyber Security Tip ST04-010.

References:

- Vulnerability Note VU#970180 - <http://www.kb.cert.org/vuls/id/970180>
- Cyber Security Tip ST04-010: Using Caution with Email Attachments - <http://www.us-cert.gov/cas/tips/ST04-010.html>
- Adobe Security Bulletin APSB09-06 - <http://www.adobe.com/support/security/bulletins/apsb09-06.html>
- CVE-2009-1492 - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1492>
- CVE-2009-1493 - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1493>