



State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

December 15, 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:

SA2009-075

DATE(S) ISSUED:

12/15/2009

12/17/2009 – UPDATED

1/13/2010 – UPDATED

SUBJECT:

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

ORIGINAL OVERVIEW:

A vulnerability discovered in the Adobe Acrobat and Adobe Reader applications could allow 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. 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 the vulnerability is being actively exploited on the Internet.

December 17, 2009 - UPDATED OVERVIEW:

Adobe has stated that they will release a patch for this vulnerability by January 12, 2010. Adobe has released information detailing a workaround to prevent the vulnerability being exploited on certain versions of Adobe Acrobat and Reader.

January 13, 2010 – UPDATED OVERVIEW

Adobe has released a patch for this vulnerability.

SYSTEMS AFFECTED:

- Adobe Acrobat Professional 9.2 and prior
- Adobe Acrobat Standard 9.2 and prior

- Adobe Reader 9.2 and prior

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

ORIGINAL DESCRIPTION:

Adobe Reader and Adobe Acrobat are prone to a remote code execution vulnerability when handling malicious PDF files. The vulnerability is found in a JavaScript function and is caused by an unspecified memory corruption error, which could be exploited by attackers to execute arbitrary code. A few anti-virus vendors are currently detecting a malicious PDF file as Trojan.Pidief.H. 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 the vulnerability is being actively exploited on the Internet.

December 17, 2009 - UPDATED DESCRIPTION:

Adobe has stated that they will release a patch for this vulnerability by January 12, 2010. Adobe has released information detailing a workaround to prevent the vulnerability being exploited on certain versions of Adobe Acrobat and Reader.

In order to employ the workaround on Windows systems, set the following registry keys (replacing '<X>' with the appropriate version number (8 or 9)):

Adobe Reader:

```
regset "[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\Acrobat Reader\<X>.0\FeatureLockDown\cJavaScriptPerms]" "tBlackList"="DocMedia.newPlayer"
```

Adobe Acrobat:

```
regset "[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\Adobe Acrobat\<X>.0\FeatureLockDown\cJavaScriptPerms]" "tBlackList"="DocMedia.newPlayer"
```

January 13, 2010 - UPDATED DESCRIPTION:

Adobe has released a patch for this vulnerability.

ORIGINAL RECOMMENDATIONS:

We recommend the following actions be taken:

- Consider disabling JavaScript in Adobe products by navigating to Edit->Preferences and unchecking 'Enable Acrobat JavaScript'.
- Ensure antivirus software signatures are current.
- Install the appropriate vendor patch as soon as it becomes available after appropriate testing.
- Do not open email attachments from unknown or un-trusted sources.
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Provide user awareness notification about this vulnerability and exploit.

December 17, 2009 - UPDATED RECOMMENDATIONS:

- Users of Adobe Reader or Acrobat versions 9.2 or 8.1.7 can utilize the Javascript Blacklist functionality noted above to prevent this vulnerability.

January 13, 2010 - UPDATED RECOMMENDATIONS:

- **Apply the appropriate patch provided by Adobe immediately after appropriate testing.**

ORIGINAL REFERENCES:**Adobe:**

http://blogs.adobe.com/psirt/2009/12/new_adobe_reader_and_acrobat_v.html

Security Focus:

<http://www.securityfocus.com/bid/37331>

Vupen:

<http://www.vupen.com/english/advisories/2009/3518>

Shadowserver:

<http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20091214>

December 17, 2009 - UPDATED REFERENCES:**Adobe:**

<http://www.adobe.com/support/security/advisories/apsa09-07.html>

January 13, 2010 - UPDATED REFERENCES:**Adobe:**

<http://www.adobe.com/support/security/bulletins/apsb10-02.html>