



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

**July 23, 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:**

7/23/09

8/3/2009 - **UPDATED**

**SUBJECT:**

Multiple Adobe Products are Prone to a Remote Code Execution Vulnerability

**ORIGINAL OVERVIEW:**

A vulnerability has been discovered in the Adobe Acrobat, Adobe Reader, and Adobe Flash Player applications that could 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. Adobe Flash Player is a multimedia and application player used to enhance the user experience when visiting web pages or reading email messages.

Exploitation can occur if a user visits a malicious webpage or opens a malicious file designed to take advantage of this vulnerability, including opening a malicious e-mail or e-mail attachment. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user account, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

There is no patch available at this time.

It should be noted that this vulnerability is being actively exploited on the Internet.

**AUGUST 3 UPDATED OVERVIEW:**

**Adobe has issued a patch for this vulnerability.**

**SYSTEMS AFFECTED:**

- Adobe Flash Player 10.0.22.87
- Adobe Flash Player 9.0.159.0
- Adobe Reader 9.x
- Adobe Acrobat 9.x

**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:**

A vulnerability has been identified in multiple Adobe products that could allow for remote code execution. The vulnerability is triggered by opening a specially crafted Flash (.swf) file or by opening a .pdf file with a malicious embedded flash application. The vulnerability affects the 'flash9f.dll' (used by Adobe Flash) and 'authplay.dll' (used by Adobe Reader 9.x and Adobe Acrobat 9.x) modules within the Adobe ActionScript Virtual Machine.

Successful exploitation may 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 user level of logged on user. Failed exploitation could result in denial-of-service conditions.

Adobe recommends disabling Flash and 3D & Multimedia support in Adobe Acrobat and Adobe Reader 9 to temporarily mitigate this vulnerability.

To disable Flash and 3D & Multimedia support in Adobe Reader 9 on Microsoft Windows, delete or rename these files:

```
"%ProgramFiles%\Adobe\Reader 9.0\Reader\authplay.dll"  
"%ProgramFiles%\Adobe\Reader 9.0\Reader\rt3d.dll"
```

To disable Flash and 3D & Multimedia support in Adobe Acrobat on Microsoft Windows, delete or rename these files:

```
"%ProgramFiles%\Adobe\Acrobat 9.0\Acrobat\authplay.dll"  
"%ProgramFiles%\Adobe\Acrobat 9.0\Acrobat\rt3d.dll"
```

The above mitigation steps will result in reduced functionality within Adobe Acrobat and Acrobat Reader applications. The file locations listed above may vary due to customized installations of Adobe Acrobat applications.

There is no patch available at this time.

It should be noted that this vulnerability is being actively exploited on the Internet.

**AUGUST 3 UPDATED DESCRIPTION:**

**A patch has been issued by Adobe for this vulnerability.**

**ORIGINAL RECOMMENDATIONS:**

We recommend the following actions be taken:

- We recommend the following actions be taken:
- Rename or delete the files listed above.
- Remind users not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not open email attachments from unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

#### **AUGUST 3 UPDATED RECOMMENDATIONS:**

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

#### **REFERENCES:**

**Adobe:**

<http://www.adobe.com/support/security/advisories/apsa09-03.html>

**Security Focus:**

<http://www.securityfocus.com/bid/35759>

**US-CERT:**

<http://www.kb.cert.org/vuls/id/259425>

**Symantec:**

<http://www.symantec.com/connect/blogs/next-generation-flash-vulnerability>

**IT-ISAC:**

<https://www.it-isac.org/postings/cyber/alertdetail.php?id=4649>

#### **AUGUST 3 UPDATED REFERENCES:**

**Adobe:**

<http://www.adobe.com/support/security/bulletins/apsb09-10.html>

**CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1862>