

State of Alaska State Security Office



State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

August 5, 2010

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:

SA2010-049

DATE(S) ISSUED:

8/5/2010

8/20/2010 - *Updated*

SUBJECT:

Multiple Adobe Products are Prone to a Remote Code Execution Vulnerability

ORIGINAL OVERVIEW:

A vulnerability has been discovered in Adobe Acrobat and Adobe Reader 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. 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.

~~There is currently no patch available for this vulnerability~~

UPDATED OVERVIEW:

Adobe has released an update which addresses this vulnerability in APSB10-17.

SYSTEMS AFFECTED:

- Adobe Acrobat Standard 9.3.3 and prior
- Adobe Acrobat Professional 9.3.3 and prior
- Adobe Reader 9.3.3 and prior
- Adobe Acrobat Reader (for Linux) 9.1.1

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 caused by an integer-overflow error in the CoolType.dll when parsing TrueType fonts (TTF). If an attacker can successfully manipulate the "maxCompositePoints" field value in the "maxp" (maximum Profile) table of a TrueType font, then a successful attack may be possible.

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.

~~There is currently no patch available for this vulnerability.~~

UPDATED DESCRIPTION:

Adobe has released an update which addresses this vulnerability in APSB10-17.

ORIGINAL RECOMMENDATIONS:

We recommend the following actions be taken:

- Install the appropriate vendor patch as soon as it becomes available after appropriate testing.
- Consider blocking PDF files at your enterprise perimeter.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

UPDATED RECOMMENDATION:

We recommend the following action be taken:

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

ORIGINAL REFERENCES:

Secunia:
<http://secunia.com/advisories/40766>

VUPEN:
<http://www.vupen.com/english/advisories/2010/2004>

Crash analysis with BitBlaze (Charlie Miller):
<http://securityevaluators.com/files/papers/CrashAnalysis.pdf>

UPDATED REFERENCES:

Adobe:
[***http://www.adobe.com/support/security/bulletins/apsb10-17.html***](http://www.adobe.com/support/security/bulletins/apsb10-17.html)