

State of Alaska State Security Office



State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

September 9, 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:
SA2010-065

DATE(S) ISSUED:

9/9/2010

10/5/2010 - *Updated*

SUBJECT:

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

ORIGINAL OVERVIEW:

A vulnerability has been discovered in the Adobe Acrobat and Adobe Reader applications which could allow attackers to execute arbitrary code on the affected systems. Adobe Reader allows users to view Portable Document Format (PDF) files while Adobe Acrobat offers users additional features such as the ability to create PDF files. This vulnerability may be exploited if a user visits or is redirected to a specially crafted web page or when a user opens a specially crafted PDF file. Successful exploitation will 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 are reports of active exploitation of this vulnerability. ~~There is currently no patch available for this vulnerability.~~

October 5 UPDATED OVERVIEW:

Adobe has released an update which addresses this vulnerability.

SYSTEMS AFFECTED:

- Adobe Acrobat 9.3.4 and earlier
- Adobe Acrobat Standard 9.3.4 and earlier
- Adobe Acrobat Professional 9.3.4 and earlier
- Adobe Reader 9.3.4 and earlier

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 exists due to a heap-memory corruption issue in 'cooltype.dll' when handling PDF files containing malformed TrueType (TTF) fonts. This vulnerability may be exploited if a user visits or is redirected to a specially crafted web page. Exploitation may also occur when a user opens a specially crafted PDF file.

Successful exploitation will 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 are reports of active exploitation of this vulnerability. ~~There is currently no patch available for this vulnerability.~~

October 5 UPDATED DESCRIPTION:

Adobe has released an update which addresses this vulnerability.

ORIGINAL RECOMMENDATIONS:

We recommend the following actions be taken:

- Install the updated software from Adobe as soon as it becomes available after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Do not open email attachments from unknown or un-trusted sources.

October 5 UPDATED RECOMMENDATIONS:

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

REFERENCES:

Adobe:

<http://www.adobe.com/support/security/advisories/apsa10-02.html>

Secunia:

<http://secunia.com/advisories/41340>

Security Focus:

<http://www.securityfocus.com/bid/43057>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2010-2883>

UPDATED REFERENCES:

Adobe:

<http://www.adobe.com/support/security/bulletins/apsb10-21.html>