

State of Alaska State Security Office



State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

August 26, 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:

SA2010-063

DATE(S) ISSUED:

8/26/2010

9/7/2010 - *Updated*

SUBJECT:

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

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.

Exploit code is publicly available. There is currently no patch available for this vulnerability.

September 7 UPDATED OVERVIEW:

Another vulnerability has been identified affecting a different part of the same application program interface, AcroForm.api, identified the original advisory. Proof of concept code has demonstrated that this new vulnerability is subject to memory corruption which could result in remote code execution.

SYSTEMS AFFECTED:

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

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

DESCRIPTION:

Adobe Reader and Adobe Acrobat are prone to a remote code execution vulnerability when handling malicious PDF files. The vulnerability is a remote memory-corruption that occurs in 'AcroForm.api' when processing unspecified 'special characters'. 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.

Exploit code is publicly available. There is currently no patch available for this vulnerability.

September 7 UPDATED DESCRIPTION:

A new vulnerability has been reported affecting the same AcroForm.api, specifically the Adobe plug-in acroform_PluginMain. This plug-in is vulnerable to a memory corruption vulnerability which could result in remote code execution.

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.

REFERENCES:

ITSecTeam:

<http://itsecteam.com/en/papers/paper11.htm>

<http://itsecteam.com/en/vulnerabilities/vulnerability62.htm>

UPDATED REFERENCES:

ITSecTeam:

<http://itsecteam.com/en/papers/paper12.htm>

<http://itsecteam.com/en/vulnerabilities/vulnerability66.htm>