State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

August 14, 2012

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.

MS-ISAC ADVISORY NUMBER:
SA2012-051

DATE (S) ISSUED:
08/14/2012

SUBJECT:
Multiple Vulnerabilities in Adobe Reader and Acrobat Could Allow For Remote Code Execution (APSB12-16)

OVERVIEW:
Multiple vulnerabilities have been discovered in Adobe Reader and Adobe Acrobat thatcould allow an attacker to take control of the affected system. 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. 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.

SYSTEMS AFFECTED:
- Adobe Reader X (10.1.3) and earlier 10.x versions for Windows and Macintosh
- Adobe Reader 9.5.1 and earlier 9.x versions for Windows and Macintosh
- Adobe Acrobat X (10.1.3) and earlier 10.x versions for Windows and Macintosh
- Adobe Acrobat 9.5.1 and earlier 9.x versions for Windows and Macintosh

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 Acrobat are prone to multiple vulnerabilities that could allow for remote code execution. Details of these vulnerabilities are as follows:

- Unspecified stacks overflow vulnerability that could lead to code execution (CVE-2012-2049).
- Unspecified buffer overflow vulnerability that could lead to code execution (CVE-2012-2050).
- Multiple unspecified memory corruption vulnerabilities that could lead to code execution (CVE-2012-2051, CVE-2012-4147, CVE-2012-4148, CVE-2012-4149, CVE-2012-4150, CVE-2012-4151, CVE-2012-4152, CVE-2012-4153, CVE-2012-4154, CVE-2012-4155, CVE-2012-4156, CVE-2012-4157, CVE-2012-4158, CVE-2012-4159, CVE-2012-4160).
- Unspecified heaps overflow vulnerability that could lead to code execution (CVE-2012-1525).
- Unspecified memory corruption vulnerability that could lead to code execution (CVE-2012-4161, CVE-2012-4162) (Macintosh only).

Successful exploitation could result in an attacker gaining the same privileges as thelogged 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.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Consider installing and running Adobe Reader X in Protected Mode.
- 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 untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.

REFERENCES:
Adobe:
http://www.adobe.com/support/security/bulletins/apsb12-16.html

Security Focus:
http://www.securityfocus.com/bid/54946

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1525
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2049
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2050
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2051
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4147
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4148
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4149
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4150
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4151
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4152
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4153
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4154
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4155
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4156

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4157
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4158
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4159
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4160
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4161
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4162