



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

September 13, 2011

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:

SA2011-053

DATE(S) ISSUED:

9/13/2011

SUBJECT:

Multiple Vulnerabilities in Adobe Reader and Acrobat Could Allow For Remote Code Execution (APSB11-24)

OVERVIEW:

Multiple vulnerabilities have been discovered in Adobe Reader and Acrobat that could allow attackers to take complete control of 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. 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) and earlier 10.x versions for Windows and Macintosh
- Adobe Reader 9.4.5 and earlier 9.x versions for Windows, Macintosh and UNIX
- Adobe Reader 8.3 and earlier 8.x versions for Windows and Macintosh
- Adobe Acrobat X (10.1) and earlier 10.x versions for Windows and Macintosh
- Adobe Acrobat 9.4.5 and earlier 9.x versions for Windows and Macintosh
- Adobe Acrobat 8.3 and earlier 8.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:

- Multiple Heap Buffer Overflow vulnerabilities that could lead to remote code execution.
- Multiple Remote Stack Buffer Overflow vulnerabilities that could lead to remote code execution
- One security bypass vulnerability that could lead to remote code execution.
- One unspecified logic error that could lead to remote code execution
- One use-after-free error vulnerability that could lead to remote code execution
- One memory leak vulnerability that could lead to remote code execution.
- One Buffer Overflow vulnerabilities that could lead to remote code execution.
- One Local Privilege Escalation vulnerability

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.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Consider installing and running Adobe Reader X in Protected Mode.
- 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/apsb11-24.html>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1353>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2431>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2432>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2433>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2434>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2435>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2436>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2437>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2438>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2439>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2440>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2441>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2442>

Security Focus:

<http://www.securityfocus.com/bid/49585>
<http://www.securityfocus.com/bid/49584>
<http://www.securityfocus.com/bid/49583>
<http://www.securityfocus.com/bid/49572>
<http://www.securityfocus.com/bid/49576>
<http://www.securityfocus.com/bid/49586>
<http://www.securityfocus.com/bid/49577>
<http://www.securityfocus.com/bid/49581>
<http://www.securityfocus.com/bid/49579>
<http://www.securityfocus.com/bid/49580>
<http://www.securityfocus.com/bid/49582>
<http://www.securityfocus.com/bid/49575>