

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is 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.

DATE(S) ISSUED:

05/14/2013

SUBJECT:

Multiple Vulnerabilities in Adobe Reader and Acrobat Could Allow For Remote Code Execution (APSB13-15)

OVERVIEW:

Multiple vulnerabilities have been discovered in Adobe Reader and Adobe Acrobat that could 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.

SYSTEM AFFECTED:

- Adobe Reader XI (11.0.02) and earlier 11.x versions for Windows and Macintosh
- Adobe Reader X (10.1.6) and earlier 10.x versions for Windows and Macintosh
- Adobe Reader 9.5.4 and earlier 9.x versions for Windows, Macintosh and Linux
- Adobe Acrobat XI (11.0.02) and earlier 11.x versions for Windows and Macintosh
- Adobe Acrobat X (10.1.6) and earlier 10.x versions for Windows and Macintosh
- Adobe Acrobat 9.5.4 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:

- Eighteen memory corruption vulnerabilities that could lead to code execution.
- An integer underflow vulnerability that could lead to code execution.
- A use-after-free vulnerability that could lead to a bypass of Adobe Reader's sandbox protection.
- An information leakage issue involving a Javascript API.
- A stack overflow vulnerability that could lead to code execution.
- A buffer overflow vulnerabilities that could lead to code execution.
- Integer overflow vulnerabilities that could lead to code execution.
- A flaw in the way Reader handles domains that have been blacklisted in the operating system.

RECOMMENDATIONS:

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Users of Adobe Reader XI (11.0.02) for Windows and Macintosh should update to Adobe Reader XI (11.0.03).
- Users of Adobe Reader X (10.1.6) and earlier versions for Windows and Macintosh, who cannot update to Adobe Reader XI (11.0.03), Adobe has made available the update Adobe Reader X (10.1.7).
- Users of Adobe Reader 9.5.4 and earlier versions for Windows and Macintosh, who cannot update to Adobe Reader XI (11.0.03), Adobe has made available the update Adobe Reader 9.5.5.
- Users of Adobe Reader 9.5.4 and earlier versions for Linux should update to Adobe Reader 9.5.5.
- Users of Adobe Acrobat XI (11.0.02) for Windows and Macintosh should update to Adobe Acrobat XI (11.0.03).
- Users of Adobe Acrobat X (10.1.6) and earlier versions for Windows and Macintosh, who cannot update to Adobe Acrobat XI (11.0.03), Adobe has made available the update Adobe Acrobat X (10.1.7).
- Users of Adobe Acrobat 9.5.4 and earlier versions for Windows and Macintosh, who cannot update to Adobe Acrobat XI (11.0.03), Adobe has made available the update Adobe Acrobat 9.5.5.
- 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/apsb13-15.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2549>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2550>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2718>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2719>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2720>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2721>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2722>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2723>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2724>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2725>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2726>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2727>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2729>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2730>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2731>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2732>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2733>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2734>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2735>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2736>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2737>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3337>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3338>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3339>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3340>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3341>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3342>