

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:

06/15/2011

SUBJECT:

Multiple Vulnerabilities in Adobe Reader and Acrobat Could Allow For Remote Code Execution (APSB11-16)

OVERVIEW:

Multiple vulnerabilities have been discovered in AdobeReader 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.

It should be noted that an exploit for one of these vulnerabilities has been included in the Metasploit project.

SYSTEMS AFFECTED:

- Adobe Reader X (10.0.1) and earlier 10.x versions for Windows
- Adobe Reader X (10.0.3) and earlier 10.x versions for Macintosh
- Adobe Reader 9.4.4 and earlier 9.x versions for Windows and Macintosh
- Adobe Reader 8.2.6 and earlier 8.x versions for Windows and Macintosh
- Adobe Acrobat X (10.0.3) and earlier 10.x versions for Windows and Macintosh
- Adobe Acrobat 9.4.4 and earlier 9.x versions for Windows and Macintosh
- Adobe Acrobat 8.2.6 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:

- Three Buffer Overflow vulnerabilities that could lead to remote code execution.
- One Heap Overflow vulnerability that could lead to remote code execution.
- Six memory corruption vulnerabilities that could lead to code execution or denial of service.
- One DLL loading vulnerability that could lead to code execution. Successful exploitation could occur when a user opens a file on a remote WebDav or SMB share. An exploit is available through the Metasploit project for this vulnerability.
- One cross document script execution vulnerability that could lead to code execution. Successful exploitation could occur when a user views a malicious website.
- One security bypass 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:

The following actions should 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/apsb11-16.html>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2094>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2095>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2096>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2097>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2098>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2099>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2100>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2101>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2102>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2103>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2104>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2105>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2106>

Security Focus:

<http://www.securityfocus.com/bid/48240>

<http://www.securityfocus.com/bid/48242>

<http://www.securityfocus.com/bid/48243>

<http://www.securityfocus.com/bid/48244>

<http://www.securityfocus.com/bid/48245>

<http://www.securityfocus.com/bid/48246>

<http://www.securityfocus.com/bid/48247>

<http://www.securityfocus.com/bid/48248>

<http://www.securityfocus.com/bid/48249>

<http://www.securityfocus.com/bid/48251>

<http://www.securityfocus.com/bid/48252>

<http://www.securityfocus.com/bid/48253>

<http://www.securityfocus.com/bid/48255>