

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 ISSUED:

05/13/2014

SUBJECT:

Multiple Vulnerabilities in Adobe Reader and Adobe Acrobat Could Allow Remote Code Execution (APSB14-15)

EXECUTIVE SUMMARY:

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. 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.

THREAT INTELLIGENCE:

At this time these vulnerabilities are not publicly disclosed and there is no known proof-of-concept code available.

SYSTEMS AFFECTED:

- Adobe Reader XI (11.0.06) and earlier 11.x versions for Windows and Macintosh
- Adobe Reader X (10.1.9) and earlier 10.x versions for Windows and Macintosh
- Adobe Acrobat XI (11.0.06) and earlier 11.x versions for Windows and Macintosh
- Adobe Acrobat X (10.1.9) and earlier 10.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

TECHNICAL SUMMARY:

Adobe Reader and Acrobat are prone to multiple vulnerabilities which could allow remote code execution, information disclosure, or security bypasses including:

- A heap overflow vulnerability which could allow remote code execution (CVE-2014-0511)
- An input validation error which could allow security bypass to take place (CVE-2014-0512)
- An issue in the implementation of JavaScript APIs could allow information disclosure (CVE-2014-0521)
- Multiple memory corruption vulnerabilities which could allow remote code execution (CVE-2014-0522, CVE-2014-0523, CVE-2014-0524, CVE-2014-0526)
- An issue with how the API handles certain calls to unmapped memory which could allow remote execution (CVE-2014-0525)
- A use-after-free vulnerability which could allow remote code execution (CVE-2014-0527)
- A double-free vulnerability which could allow remote code execution (CVE-2014-0528)
- A buffer overflow vulnerability which could allow remote code execution (CVE-2014-0529)

Successful exploitation of these vulnerabilities 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 result in denial-of-service conditions.

RECOMMENDATIONS:

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.
- Limit user account privileges to those required only.

REFERENCES:

ADOBE:

<http://helpx.adobe.com/security/products/reader/apsb14-15.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0511>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0512>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0521>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0522>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0523>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0524>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0525>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0526>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0527>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0528>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0529>