

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:

12/09/2014

SUBJECT:

Multiple Vulnerabilities in Adobe Reader and Adobe Acrobat Could Allow Remote Code Execution (APSB14-28)

OVERVIEW:

Multiple vulnerabilities have been discovered in Adobe Reader and Adobe Acrobat. Adobe Reader and Acrobat are applications for handling PDF files.

Attackers can exploit these issues to execute arbitrary code within the context of the affected application. Successful exploitation could result in an attacker compromising data security, potentially allowing access to confidential data, or could compromise processing resources in a user's computer. Failed exploit attempts will likely cause denial-of-service conditions.

THREAT INTELLIGENCE

There are currently no reports of these vulnerabilities being exploited in the wild. There are no known exploits for these vulnerabilities.

SYSTEM AFFECTED:

Adobe Reader XI (11.0.09) and earlier 11.x versions
Adobe Reader X (10.1.12) and earlier 10.x versions
Adobe Acrobat XI (11.0.09) and earlier 11.x versions
Adobe Acrobat X (10.1.12) and earlier 10.x versions

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:**

Multiple vulnerabilities have been discovered in Adobe Reader and Adobe Acrobat that could potentially allow an attacker to take over the affected system. Adobe recommends users update their product installations to the latest versions. These updates resolve:

- A use-after-free vulnerabilities that could lead to code execution (CVE-2014-8454, CVE-2014-8455, CVE-2014-9165)
- A heap-based buffer overflow vulnerabilities that could lead to code execution (CVE-2014-8457, CVE-2014-8460, CVE-2014-9159)
- An integer overflow vulnerability that could lead to code execution (CVE-2014-8449)
- A memory corruption vulnerabilities that could lead to code execution (CVE-2014-8445, CVE-2014-8446, CVE-2014-8447, CVE-2014-8456, CVE-2014-8458, CVE-2014-8459, CVE-2014-8461, CVE-2014-9158)
- A time-of-check time-of-use (TOCTOU) race condition that could be exploited to allow arbitrary write access to the file system (CVE-2014-9150)
- An improper implementation of a Javascript API that could lead to information disclosure (CVE-2014-8448, CVE-2014-8451)
- A vulnerability in the handling of XML external entities that could lead to information disclosure (CVE-2014-8452)
- A vulnerabilities that could be exploited to circumvent the same-origin policy (CVE-2014-8453)

Successful exploitation could result in an attacker compromising data security, potentially allowing access to confidential data, or could compromise processing resources in a user's computer. 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.
- 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.
Limit user account privileges to only those required by job function.

REFERENCES:

Adobe:

<http://helpx.adobe.com/security/products/flash-player/apsb14-28.html>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9165>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8445>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9150>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8446>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8447>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8448>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8449>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8451>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8452>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8453>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8454>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8455>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8456>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8457>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8458>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8459>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8460>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8461>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9158>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9159>