

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.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp>

DATE(S) ISSUED:

05/12/2015

SUBJECT:

Multiple Vulnerabilities in Adobe Reader and Adobe Acrobat Could Allow Remote Code Execution (APSB15-10)

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.

SYSTEM AFFECTED:

- Adobe Reader XI (11.0.10) and earlier 11.x versions
- Adobe Reader X (10.1.13) and earlier 10.x versions
- Adobe Acrobat XI (11.0.10) and earlier 11.x versions
- Adobe Acrobat X (10.1.13) 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.

- Use-after-free vulnerabilities that could lead to code execution (CVE-2015-3053, CVE-2015-3054, CVE-2015-3055, CVE-2015-3059, CVE-2015-3075)
- A heap-based buffer overflow vulnerability that could lead to code execution (CVE-2014-9160)
- A buffer overflow buffer overflow vulnerability that could lead to code execution (CVE-2015-3048)
- Memory corruption vulnerabilities that could lead to code execution (CVE-2014-9161, CVE-2015-3046, CVE-2015-3049, CVE-2015-3050, CVE-2015-3051, CVE-2015-3052, CVE-2015-3056, CVE-2015-3057, CVE-2015-3070, CVE-2015-3076)
- Addresses a memory leak issue (CVE-2015-3058)
- Various security bypass vulnerabilities for the JavaScript API (CVE-2015-3060, CVE-2015-3061, CVE-2015-3062, CVE-2015-3063, CVE-2015-3064, CVE-2015-3065, CVE-2015-3066, CVE-2015-3067, CVE-2015-3068, CVE-2015-3069, CVE-2015-3071, CVE-2015-3072, CVE-2015-3073, CVE-2015-3074)
- A null-pointer dereference pointer vulnerability which could cause denial of service conditions (CVE-2015-3047)
- A vulnerability that could be exploited to circumvent the same-origin policy (CVE-2014-8453)
- These updates provide additional hardening to protect against CVE-2014-8452, which is a vulnerability in the handling of XML external entities that could lead to information disclosure.

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.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Adobe:

<https://helpx.adobe.com/security/products/reader/apsb15-10.html>

CVE:

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

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9160>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9161>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3046>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3047>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3048>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3049>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3050>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3051>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3052>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3053>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3054>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3055>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3056>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3057>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3058>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3059>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3060>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3061>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3062>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3063>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3064>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3065>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3066>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3067>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3068>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3069>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3070>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3071>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3072>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3073>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3074>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3075>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3076>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>