

*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:**

01/12/2016

**SUBJECT:**

Multiple Vulnerabilities in Adobe Acrobat and Adobe Reader Could Allow for Remote Code Execution (APSB16-02)

**OVERVIEW:**

Multiple vulnerabilities in Adobe Acrobat and Adobe Reader could allow for remote code execution. Adobe Acrobat and Reader allow a user to view, create, manipulate, print and manage files in Portable Document Format (PDF). Successful exploitation could potentially allow an attacker to take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full system rights.

**THREAT INTELLIGENCE**

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

**SYSTEMS AFFECTED:**

- Adobe Acrobat DC version prior to 15.010.20056 for Windows and Macintosh
- Acrobat Reader DC version prior to 15.010.20056 for Windows and Macintosh
- Acrobat DC version prior to 15.006.30119 for Windows and Macintosh
- Adobe Acrobat Reader DC version prior to 15.006.30119 for Windows and Macintosh
- Adobe Acrobat XI version prior to 11.0.14 Windows and Macintosh
- Adobe Reader XI version prior to 11.0.14 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 Acrobat and Reader are prone to multiple vulnerabilities. These vulnerabilities are as follows:

- Multiple use-after-free vulnerabilities exist that could lead to code execution (CVE-2016-0932, CVE-2016-0934, CVE-2016-0937, CVE-2016-0940, CVE-2016-0941).
- A double-free vulnerability exists that could lead to code execution (CVE-2016-0935).

- Multiple memory corruption vulnerabilities exist that could lead to code execution (CVE-2016-0931, CVE-2016-0933, CVE-2016-0936, CVE-2016-0938, CVE-2016-0939, CVE-2016-0942, CVE-2016-0944, CVE-2016-0945, CVE-2016-0946).
- Bypass restrictions on JavaScript API execution (CVE-2016-0943).
- Directory search path used to find resources that could lead to code execution (CVE-2016-0947).
- Successful exploitation could potentially allow an attacker to take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full system rights.

#### **RECOMMENDATIONS:**

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Do not open email attachments from unknown or untrusted sources.
- 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 un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

#### **REFERENCES:**

##### **Adobe**

<https://helpx.adobe.com/security/products/reader/apsb16-02.html>

##### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0931>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0932>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0933>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0934>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0935>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0936>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0937>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0938>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0939>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0940>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0941>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0942>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0943>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0944>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0945>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0946>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0947>

#### **TLP: WHITE**

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

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