

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:

08/25/2016

09/19/2016 - UPDATED

SUBJECT:

Multiple Vulnerabilities in Adobe Acrobat and Adobe Reader Could Allow for Arbitrary Code Execution (APSB16-26)

OVERVIEW:

Multiple vulnerabilities in Adobe Acrobat and Adobe Reader could allow for arbitrary 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.

September 19 - UPDATED OVERVIEW:

Two additional vulnerabilities have been reported in Adobe Flash Player which could allow for arbitrary code execution.

THREAT INTELLIGENCE:

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

SYSTEM AFFECTED:

- Adobe Acrobat DC version 15.016.20045 and prior for Windows and Macintosh
- Acrobat Reader DC version 15.016.20045 and prior for Windows and Macintosh
- Acrobat DC version 15.006.30174 and prior for Windows and Macintosh
- Adobe Acrobat Reader DC version 15.006.30174 and prior for Windows and Macintosh
- Adobe Acrobat XI version 11.0.16 and prior Windows and Macintosh
- Adobe Reader XI version 11.0.16 and prior for Windows and Macintosh

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

Adobe Acrobat and Reader are prone to multiple vulnerabilities, the most severe of which could allow for arbitrary code execution. The vulnerabilities are as follows:

- Integer overflow vulnerability that could lead to code execution (CVE-2016-4210).
- Use-after-free vulnerability that could lead to code execution (CVE-2016-4255).
- Heap buffer overflow vulnerability that could lead to code execution (CVE-2016-4209).
- Bypass restrictions on Javascript API execution (CVE-2016-4215).
- Memory corruption vulnerabilities that could lead to code execution (CVE-2016-4254, CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, CVE-2016-4265, CVE-2016-4266, CVE-2016-4267, CVE-2016-4268, CVE-2016-4269, CVE-2016-4270).

The most severe of these vulnerabilities could allow an attacker to execute arbitrary code. An attacker could then install programs; view, change, or delete data; or create new accounts with full system rights.

September 19 - UPDATED TECHNICAL SUMMARY:

Adobe Acrobat and Reader are prone to a memory corruption vulnerability (CVE-2016-6937) and a use-after-free vulnerability (CVE-2016-6938). Successful exploitation of these vulnerabilities could allow for arbitrary code execution.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Adobe to vulnerable systems 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 visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from untrusted sources.

REFERENCES:

Adobe:

<https://helpx.adobe.com/security/products/acrobat/apsb16-26.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4191>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4192>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4193>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4194>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4195>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4196>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4197>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4198>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4199>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4200>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4201>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4202>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4203>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4204>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4205>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4206>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4207>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4208>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4209>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4210>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4211>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4212>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4213>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4214>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4215>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4250>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4251>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4252>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4254>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4255>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4265>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4266>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4267>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4268>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4269>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4270>

September 19 - UPDATED REFERENCES:

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6937>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6938>

TLP: WHITE

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

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