

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/tp/>

DATE(S) ISSUED:

07/12/2016

SUBJECT:

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

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 no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Adobe Acrobat DC version prior to 15.016.20045 for Windows and Macintosh
- Acrobat Reader DC version prior to 15.016.20045 for Windows and Macintosh
- Acrobat DC version prior to 15.006.30174 for Windows and Macintosh
- Adobe Acrobat Reader DC version prior to 15.006.30174 for Windows and Macintosh
- Adobe Acrobat XI version prior to 11.0.16 Windows and Macintosh
- Adobe Reader XI version prior to 11.0.16 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 remote code execution. The vulnerabilities are as follows:

- Integer overflow vulnerability that could lead to code execution (CVE-2016-4210).
- Vulnerability that could lead to code execution (CVE-2016-4190).
- 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-2016-4189, 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).

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.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Limit user account privileges to those required only.
- Do not open email attachments from unknown or 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-2016-4189>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4190>
<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-2016-4189>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4190>
<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>

TLP: WHITE

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

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