

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:

10/11/2016

SUBJECT:

Multiple Vulnerabilities in Adobe Flash Player Could Allow for Remote Code Execution (APSB16-32)

OVERVIEW:

Multiple vulnerabilities have been discovered in Adobe Flash Player, the most severe of which could allow for remote code execution. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute remote code by luring a victim to visit a specially crafted malicious website. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. Failed attacks may cause a denial-of-service condition.

THREAT INTELLIGENCE:

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

SYSTEMS AFFECTED:

- Adobe Flash Player Desktop Runtime prior to version 23.0.0.185
- Adobe Flash Player Extended Support Release prior to version 18.0.0.382
- Adobe Flash Player for Google Chrome prior to version 23.0.0.185
- Adobe Flash Player for Microsoft Edge and Internet Explorer 11 prior to version 23.0.0.185
- Adobe Flash Player for Linux prior to version 11.2.202.637

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 Flash Player is prone to multiple vulnerabilities which could allow an attacker to take control of the affected system.

- A type confusion vulnerability that could lead to code execution (CVE-2016-6992).
- A Use-after-free vulnerabilities that could lead to code execution (CVE-2016-6981, CVE-2016-6987).
- A security bypass vulnerability (CVE-2016-4286).
- Multiple memory corruption vulnerabilities that could lead to code execution (CVE-2016-4273, CVE-2016-6982, CVE-2016-6983, CVE-2016-6984, CVE-2016-6985, CVE-2016-6986, CVE-2016-6989, CVE-2016-6990).

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute remote code by luring a victim to visit a specially crafted malicious website. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. Failed attacks may result in a denial-of-service condition.

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.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Adobe:

<https://helpx.adobe.com/security/products/flash-player/apsb16-32.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4273>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4286>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6981>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6982>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6983>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6984>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6985>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6986>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6987>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6989>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6990>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6992>

TLP: WHITE

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

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

