

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:

07/12/2015

SUBJECT:

Vulnerability in Adobe Flash Player ActionScript 3 Could Allow for Arbitrary Code Execution (APSA15-04)

OVERVIEW:

A vulnerability has been discovered in Adobe Flash Player which could allow arbitrary 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 this vulnerability could result in an attacker executing arbitrary code in the context of the user running the affected applications. 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. A failed exploit attempt could create a denial-of-service attack.

THREAT INTELLIGENCE:

Proof of Concept code is publicly available. Adobe is aware of reports of this vulnerability being exploited in the wild.

SYSTEM AFFECTED:

- Adobe Flash Player 18.0.0.203 and earlier for Windows and Macintosh
- Adobe Flash Player 18.0.0.204 and earlier for Linux installed with Google Chrome
- Adobe Flash Player Extended Support Release 13.0.0.302 and earlier for Windows and Macintosh
- Adobe Flash Player Extended Support Release 11.2.202.481 and earlier for Linux

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:

A use after free vulnerability exists in the way Adobe Flash Player ActionScript 3 handles the 'opaqueBackground' class. A use after free vulnerability occurs when a memory location is referenced after it has been freed. This attack can be executed using two different attack vectors. The first is done by creating a malicious Flash file which is then distributed to the user

using email or other such method. The second is done by crafting a malicious web page to which the user is then redirected using social engineering. An attacker utilizing this vulnerability can run arbitrary code in the context of the user running the affected application.

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. A failed attack can still cause a denial of service attack by causing the affected program to crash.

RECOMMENDATIONS:

The following actions should be taken:

- Once a patch is released by Adobe, update 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 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/flash-player/apsa15-04.html>

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5122>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5123>

TLP: WHITE

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

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