

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:

09/08/2015

SUBJECT:

Multiple Vulnerabilities in Adobe Shockwave Player Could Allow for Remote Code Execution (APSB15-22)

OVERVIEW:

Two vulnerabilities have been discovered in Adobe Shockwave Player, which could allow for arbitrary code execution. Adobe Shockwave Player is a multimedia platform used to add animation and interactivity to web pages.

Successful exploitation of these vulnerabilities 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:

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

SYSTEM AFFECTED:

- Adobe Shockwave Player 12.1.9.160 and earlier for Microsoft Windows

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:

Two memory corruption vulnerabilities exist in the way Adobe Shockwave Player accesses objects in memory. These vulnerabilities can be exploited by using two different attack vectors. The first is done by creating a malicious Shockwave 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 to using social engineering. An attacker utilizing this vulnerability can run 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. Failed attacks can result in a denial of service condition.

RECOMMENDATIONS:

The following actions should be taken:

- Apply available patch from Adobe 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/shockwave/apsb15-22.html>

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6680>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6681>

TLP: WHITE

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

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