

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:

10/27/2015

SUBJECT:

A Vulnerability has been Discovered in Adobe Shockwave Player that Could Allow for Arbitrary Code Execution (APSB15-26)

OVERVIEW:

An Unspecified Memory Corruption Vulnerability has been discovered in Adobe Shockwave Player, which could allow for an attacker to execute arbitrary code or crash the application. Adobe Shockwave Player is a multimedia platform used to add animation and interactivity to web pages.

Successfully exploiting this vulnerability may allow an attacker to execute arbitrary code within the context of the user running the affected application. Failed attempts will likely cause a denial-of-service condition.

THREAT INTELLIGENCE

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

SYSTEM AFFECTED:

- Adobe Shockwave Player prior to 12.2.1.171

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:

An Unspecified Memory Corruption Vulnerability has been discovered in Adobe Shockwave Player, which could allow for an attacker to execute arbitrary code or crash the application. The vulnerability can be exploited by the attacker crafting a malicious Shockwave file and attaching it to an email or creating a malicious webpage the user interacts with.

Successfully exploiting this vulnerability may allow an attacker to 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. 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/apsb15-26.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7649>

TLP: WHITE

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

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