

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:

01/12/2016

SUBJECT:

Vulnerability in Microsoft Silverlight Could Allow Remote Code Execution (MS16-006)

OVERVIEW:

A vulnerability has been discovered in Microsoft Silverlight, which could allow for remote code execution. Microsoft Silverlight is a media application for browsers on Microsoft Windows and Apple Mac OS technologies. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

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

SYSTEMS AFFECTED:

- Microsoft Silverlight 5 prior to version 5.1.41212.0 for Windows Clients, Windows Servers, and Mac
- Microsoft Silverlight 5 Developer Runtime prior to version 5.1.41212.0 for Windows Clients, Windows Servers, and Mac

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:

One vulnerability has been discovered in Microsoft Silverlight, which could allow for remote code execution (CVE-2016-0034). This vulnerability exists when Microsoft Silverlight decodes strings using a malicious decoder that can return negative offsets that cause Silverlight to replace unsafe object headers with contents provided by an attacker. To exploit the vulnerability, an attacker could host a website that contains a specially crafted Silverlight application and then convince a user to visit the compromised website. An attacker would have no way to force users to visit a compromised website.

Instead, an attacker would have to convince a user to visit the website, typically by enticing them to click a link in an email or instant message.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate update provided by Microsoft to vulnerable systems 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:

Microsoft:

<https://technet.microsoft.com/en-us/library/security/ms16-006.aspx>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0034>

TLP: WHITE

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

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