

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:

04/12/2016

SUBJECT:

A Vulnerability in Microsoft XML Core Services Could Allow for Remote Code Execution (MS16-040)

OVERVIEW:

A vulnerability has been discovered in Microsoft XML Core Services that could allow for remote code execution. Microsoft XML Core Services is an application for processing Extensible Stylesheet Language Transformation (XSLT) in an XML file and these services are included in various Windows operating system installations, by default. 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 no reports of this vulnerability being exploited in the wild.

SYSTEM AFFECTED:

- Windows Vista
- Windows 7
- Windows 8.1
- Windows 10
- Windows Server 2008, 2008 R2 (Including Server Core Installations)

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:

A vulnerability in Microsoft XML Core Services (MSXML) exists when the MSXML parser processes user input. In an attack scenario, an attacker could host a specially-crafted website that is designed to invoke MSXML through Internet Explorer. An attacker would then have to entice a user to follow a malicious

link to the specially crafted website in order to exploit this vulnerability (CVE-2016-0147). 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.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches 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/ms16-040>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0147>

TLP: WHITE

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

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