

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:

07/20/2015

SUBJECT:

Vulnerability in Microsoft Font Driver Could Allow Remote Code Execution (MS15-078)

OVERVIEW:

A vulnerability has been discovered in Microsoft Font Drivers that could allow remote code execution. 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 reports of CVE-2015-2426 being exploited in the wild.

SYSTEM AFFECTED:

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server Core
- Windows RT
- Windows RT 8.1
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1

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:

Microsoft has released a security update that addresses a vulnerability in Microsoft Windows Font Driver that could allow for remote code execution (CVE-2015-2426). A vulnerability exists

when the Windows Adobe Type Manager Library improperly handles specially crafted fonts which can be triggered when a user opens a specially crafted document or visits an untrusted website that contains embedded OpenType fonts.

Successful exploitation could allow an attacker to gain 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 those from un-trusted sources.
- Workaround options are also available via the Microsoft link listed in the reference section

REFERENCES:

Microsoft:

<https://technet.microsoft.com/en-us/library/security/MS15-078>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2426>

TLP: WHITE

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

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