

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:

05/12/2015

SUBJECT:

Multiple Vulnerabilities in Microsoft Font Drivers Could Allow Remote Code Execution (MS15-044)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Font Drivers that could allow remote code execution. Successful exploitation of these vulnerabilities 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:

- Windows Server 2003
- Windows Vista
- Windows Server 2008 (including Server Core Installations)
- Windows 7
- Windows 8
- Windows 8.1
- Windows Server 2012 (including Server Core Installations)
- Windows RT
- Windows RT 8.1
- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Live Meeting 2007 Console
- Microsoft Lync 2010
- Microsoft Lync 2010 Attendee
- Microsoft Lync 2013
- Microsoft Lync Basic 2013
- Microsoft Silverlight 5 for Windows and MAC OS
- Microsoft Silverlight 5 Developer Runtime for Windows and MAC OS

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:

Multiple vulnerabilities in Microsoft Font Drivers could allow remote code execution.

A remote code execution vulnerability exists when components of Windows fail to properly handle TrueType fonts (CVE-2015-1671). This vulnerability can be triggered when a user opens a specially crafted document or visits an untrusted website that contains embedded TrueType fonts.

An information disclosure vulnerability exists when components of Windows fail to properly handle OpenType fonts (CVE-2015-1670). This vulnerability can be triggered when a user visits an untrusted website that contains embedded OpenType fonts.

Successful exploitation of these vulnerabilities could result in an attacker executing arbitrary code in the context of the logged on user. Depending on the privileges associated with this 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/library/security/MS15-044>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1670>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1671>

TLP: WHITE

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

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