

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:

Multiple Vulnerabilities in Microsoft Graphic Fonts Could Allow for Remote Code Execution (MS16-039)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Windows, the most severe of which could allow for remote code execution. These vulnerabilities can be exploited by either convincing a user to open a specially crafted document, convincing a user to visit a webpage that contains specially crafted embedded fonts, or by running a malicious application. 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:

Privilege escalation vulnerabilities CVE-2016-0165 and CVE-2016-0167 have been observed being exploited in the wild.

SYSTEMS AFFECTED:

- Windows Vista
- Windows Server 2008, 2008 R2 (Including Server Core installations)
- Windows 7
- Windows 8.1, RT 8.1
- Windows Server 2012, 2012 R2 (Including Server Core installations)
- Windows 10
- Microsoft Office 2007 & 2010
- Microsoft Lync 2010 & 2013
- Microsoft Word Viewer
- Microsoft Live Meeting 2007 Console
- Microsoft Skype for Business 2016

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:

Multiple vulnerabilities exist in Microsoft Windows, the most severe of which could allow remote code execution. The vulnerabilities are as follows:

- A memory corruption vulnerability exists in Microsoft Windows when improperly handling specially crafted fonts that could allow for remote code execution (CVE-2016-0145).
- Multiple privilege escalation vulnerabilities exist in all supported versions of Microsoft Windows, due to improper handling of objects in memory that could allow for arbitrary code execution. These vulnerabilities require an attacker to log on to the system before being exploited. (CVE-2016-0143, CVE-2016-0165, CVE-2016-0167)

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.

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 untrusted sources.

REFERENCES:

Microsoft:

<https://technet.microsoft.com/en-us/library/security/ms16-039>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0143>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0145>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0165>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0167>

TLP: WHITE

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

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