

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:

12/08/2015

SUBJECT:

Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (MS15-128)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Windows operating systems and applications that could allow for 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 no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

- Windows Vista
- Windows 7
- Windows Server 2008, R2, and Server Core Installation
- Windows Server 2012, R2, and Server Core Installation
- Windows RT, RT 8.1
- Windows 8, 8.1
- Windows 10
- Office 2007, 2010
- Skype for Business 2016
- Lync 2010, 2013
- Live Meeting 2007
- Silverlight 5, Silverlight Developer

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:

Three memory corruption vulnerabilities were discovered in Microsoft Windows operating systems and applications that could allow for remote code execution. The vulnerabilities exist in how the Windows font

library improperly handles specially crafted embedded fonts (CVE-2015-6106, CVE-2015-6107, CVE-2015-6108).

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.
- Do not visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.

REFERENCES:

Microsoft:

<https://technet.microsoft.com/en-us/library/security/ms15-128.aspx>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2015-6106>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2015-6107>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2015-6108>

TLP: WHITE

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

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