

*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:**

Vulnerability in Microsoft Uniscribe Could Allow Remote Code Execution (MS15-130)

**OVERVIEW:**

A vulnerability exists in Windows Uniscribe that could allow for remote code execution. Uniscribe is a set of APIs that allow a high degree of control for fine typography and for processing complex scripts as well as supports the display and editing of international text. 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:**

- Microsoft Windows 7
- Microsoft Windows Server 2008, R2, and Server Core installations

**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:**

A remote code execution vulnerability exists when Windows Uniscribe improperly parses specially crafted fonts. Uniscribe is present on current and unsupported legacy operating systems. In order to exploit this vulnerability an attacker would have to convince a user to open a specially crafted document, or visit an untrusted webpage that contains embedded fonts.

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 those from un-trusted sources.

**REFERENCES:**

Microsoft:

<https://technet.microsoft.com/library/security/MS15-130>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6130>

**TLP: WHITE**

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

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