

*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:**

Multiple Vulnerabilities in Windows Media Center Could Allow Remote Code Execution (MS15-134)

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Microsoft Windows Media Center. The most severe of these vulnerabilities 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 currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEM AFFECTED:**

- Windows Vista
- Windows 7
- Windows 8 and 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:**

Two vulnerabilities exist in Windows Media Center. The most severe of these vulnerabilities could allow for remote code execution (CVE-2015-6131). This vulnerability exists in how Windows Media Center handles specially crafted Media Center link (.mcl) files. In order to exploit this vulnerability an attacker would have to convince a user to open a specially crafted ".mcl" file, or visit an untrusted webpage hosting a malicious ".mcl" file. 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.

Details of the other vulnerability included in this update is as follows:

- An information disclosure vulnerability exists that could disclose local file system information. (CVE-2015-6127)

**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/en-us/library/security/ms15-134.aspx>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6127>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6131>

**TLP: WHITE**

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

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