

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:

05/10/2016

SUBJECT:

Vulnerability in Windows Media Center Could Allow for Remote Code Execution (MS16-059)

OVERVIEW:

A vulnerability has been discovered in Microsoft Windows Media Center, which could allow for 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:

There are no reports of this vulnerability being exploited in the wild.

SYSTEM AFFECTED:

- Windows Vista Service Pack 2
- Windows 7
- Windows 8.1

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:

A vulnerability has been discovered in Microsoft Windows Media Center, which could allow for remote code execution. 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Backup and subsequently delete the registry keys for .MCL in HKEY_CLASSES_ROOT and HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts. A managed deployment script is also available in the linked security bulletin. This is a work around to be used only if not applying the patch provided by Microsoft.
- 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/MS16-059>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0185>

TLP: WHITE

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

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