3 days ago Exploiting CVE-2015-2509 /MS15-100 : Windows Media Center could allow remote code execution

Trend Micro blog about it [http://blog.trendmicro.com/trendlabs-security-intelligence/windows-media-center-hacking-team-bug-fixed-in-september-2015-patch-tuesday/] few days ago. This vulnerability is related to Hacking Team leaked email addresses . The issue is so trival that exploitation is a piece of cake.

Vulnerability in Windows Media Center Could Allow Remote Code Execution (3087918)

Published: September 8, 2015

Version: 1.0

Executive Summary

This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if Windows Media Center opens a specially crafted Media Center link (.mcl) file that references malicious code. An attacker who successfully exploited this vulnerability could gain the same user rights as the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

This security update is rated Important for all supported editions of Windows Media Center when installed on Windows Vista, Windows 7, Windows 8, or Windows 8.1. For more information, see the **Affected Software** section.

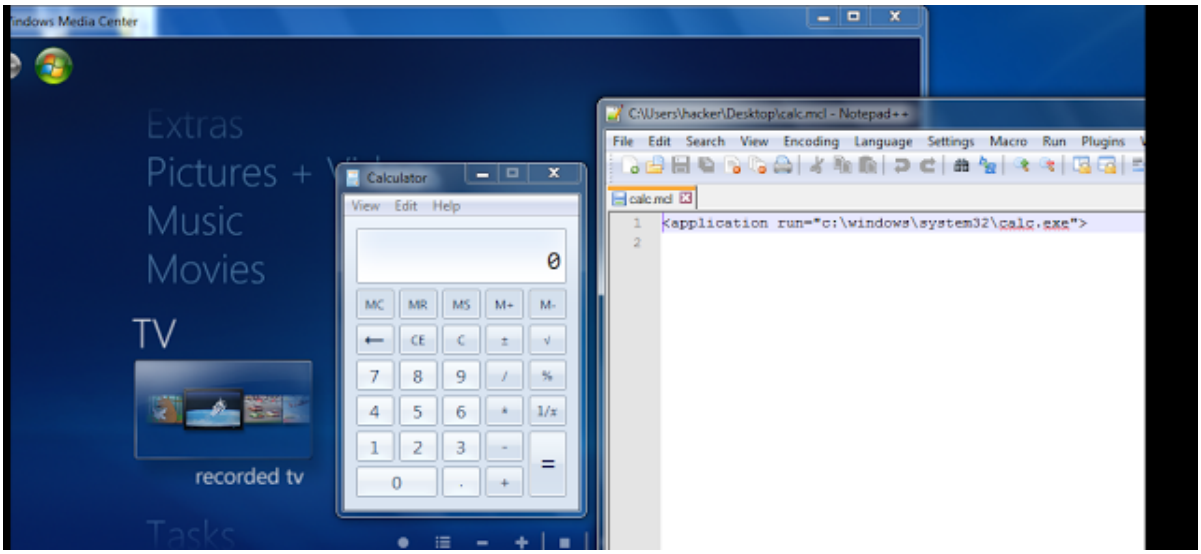
The security update addresses the vulnerability by correcting how Windows Media Center link files are handled. For more information about the vulnerability, see the **Vulnerability Information** section.

For more information about this update, see Microsoft Knowledge Base Article 3087918.

[http://4.bp.blogspot.com/-VwjAaprai94/VfJG-GQ0DrI/AAAAAAAACII/56SCngbnRJk/s1600/shit.PNG]

Source: https://technet.microsoft.com/en-us/library/security/ms15-100

Based on POC and description we just need to create a simple mcl file contains our executable path and preso it works.

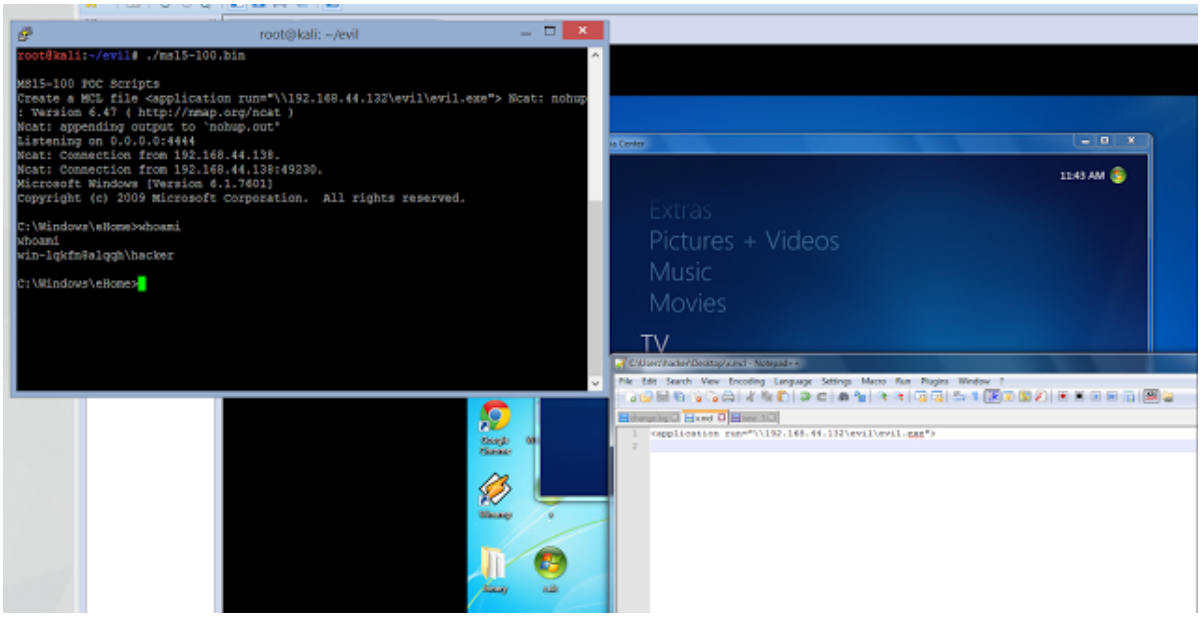


[http://1.bp.blogspot.com/-H5m2LAVLEAs/VfJI8srgjyI/AAAAAAAACIU/ZSnybZWH3Kw/s1600/shit2.PNG]

The caveat for this attack is that you cannot passed an argument such as cmd.exe /c ipconfig in the mcl file. However we can execute our payload externally via UNC PATH provided by a simple SMB Server. The steps required.

1. Generate evil payload exe
2. Setup a SMB Listener
3. Create MCL file that points to evil payload.
4. Profits.

I use Impacket SMB Server [http://www.coresecurity.com/corelabs-research/open-source-tools/impacket] to simulate the steps above. If you are a bit creative, we can use DLL Hijacking Method to cloak our payload .



[http://2.bp.blogspot.com/-YTJUPOkt0IA/VfJOYUBTfAI/AAAAAAAACIg/-V3aYwVgGRE/s1600/shit3.PNG]

Better patch it up fast.

Posted 3 days ago by Shahriman Sam

Labels: MS15-100. CVE-2015-2059, Windows Media Centr.

2 View comments

2 comments

Add a comment as NewTime AgeFul

Top comments

m10 13 hours ago - Shared publicly

Exploiting MS15-100 **#Windows #Media** Center Remote Code Execution http://buff.ly/1i8AG8b **#hacking #infosec**

1 · Reply

Shahriman Sam via Google+ 3 days ago - Shared publicly

Exploiting CVE-2015-2509 /MS15-100 : Windows Media Center could allow remote code execution
Trend Micro blog about it few days ago. This vulnerability is related to Hacking Team leaked email addresses . The issue is so trival that exploitation is a piece of cake.
Source: https://technet.microsoft.com/en-us/library/security/ms15-100 Based on POC ...

1 · Reply