

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\]Using the mod_isapi apache 2.2.14 exploit\[TUTORIAL\]](#)

TeMk - July 16, 2011, 9:18 am

Hello,

There are no Tutorials how to use this exploit. And i saw a lot of people wants to know this works. Well i will explain everything in this Tutorial.

FIRST:

I'm talking about this exploit:

[Video: <http://www.youtube.com/watch?v=m43Tz414d0Y>]

You needs:

Visual C++ 2010 -

<http://www.microsoft.com/visualstudio/en-us/products/2010-editions/visual-cpp-express>

C/C++ Command Prompt Compiler - http://www.speedyshare.com/files/29450799/dm852c_2_.zip

PuTTY or Telnet - <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

Apache 2.2.14 mod_isapi exploit -

<http://www.senseofsecurity.com.au/advisories/SOS-10-002-pwn-isapi.cpp>

Some questions:

I have Windows 7, and i want to use Telnet. How can i do that?

There is a great Tutorial about that. Just click here:

<https://hackforums.net/showthread.php?tid=1274185&highlight=Telnet+windows+7>

Begin:

Ok, if you installed/downloaded everything. I will tell what you need to do.

1 > Make a folder in C:/ called "whateveryouwant" and extract dm852c.zip.

2 > Click on Start and search for: Visual Studio Command Prompt.

3 > Open it and go to the directory where dm852c.zip was extracted, you need to go to the bin. Like this:

PHP Code

```
<?php
```

```
cd C:\whateveryouwant\bin
```

4 > Download the exploit and copy that to the bin folder. Now go to the Visual Studio Command Prompt and write this:

PHP Code

```
<?php
```

```
cl pwn-isapi.cpp
```

(can be different look at the name

The exploit will now be written, and it will be a .exe (Executable) file.

5 > Alright, now type in Visual Studio Command prompt this:

PHP Code

```
<?php
```

```
pwn-isapi.exe IPADRES "SMTPSend.dll?Send"
```

I hope you like this, and hope it will work for some people that didnt know how to do this.

Waves'
TeMk

saawan - July 16, 2011, 10:13 am

I cant understand whats in this tutorial

TeMk - July 16, 2011, 10:17 am

(Jul 16, 2011 10:13 AM)saawan Wrote: [\[CITE\]](#) I cant understand whats in this tutorial
Look at the video and you will understand what i mean.

Fa?e - July 16, 2011, 11:24 am

I've tried this before on a Windows Server 2008, but couldn't find a shellcode to work for that Operating System :(

<http://www.senseofsecurity.com.au/advisories/SOS-10-002-pwn-isapi.cpp>

Doesn't really help you gain access to the computer you are trying to exploit, all it does is this:
//custom shellcode that writes "pwn-isapi" to "sos.txt" in the current working directory
//Note: There are four NOPs at the end for padding. Not really needed.

But nonetheless, its a good proof of concept.

bombasschicken - July 16, 2011, 12:55 pm

(Jul 16, 2011 09:18 AM)TeMk Wrote: [\[CITE\]](#) You needs:
Visual C++ 2010 -

<http://www.microsoft.com/visualstudio/en-us/products/2010-editions/visual-cpp-express>

C/C++ Command Prompt Compiler - http://www.speedyshare.com/files/29450799/dm852c_2_.zip

PuTTY or Telnet - <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

Apache 2.2.14 mod_isapi exploit -

<http://www.senseofsecurity.com.au/advisories/SOS-10-002-pwn-isapi.cpp>

Some questions:

I have Windows 7, and i want to use Telnet. How can i do that?

There is a great Tutorial about that. Just click here:

<https://hackforums.net/showthread.php?tid=1274185&highlight=Telnet+windows+7>

Or just use linux and save yourself the headache..

code was proly disabled anyways..

Broomop - February 19, 2012, 7:58 am

im trying to use this on a windows 2008 if i can exploit it with help ill send some money through paypal for you.

nothing1 - February 19, 2012, 8:25 am

Was this leechd or something? He only has 2 posts, and now a closed account.

d00m - March 3, 2012, 12:13 pm

well i tried it says check for sos.txt :S what does tht mean i checked site like www.site.com/sos.txt
nothing was there and no telnet sucess too

mands - April 10, 2013, 2:16 am

sure there's no telnet connection, you need to put another payload / shellcode in the exploit.
the shellcode in exploit only writes sos.txt into the working directory.

i'll think you can put another shellcode in this exploit.

I R PK3R - April 10, 2013, 9:36 am

(Apr 10, 2013 02:16 AM)mands Wrote: [\[CITE\]](#) sure there's no telnet connection, you need to put another payload / shellcode in the exploit.
the shellcode in exploit only writes sos.txt into the working directory.

i'll think you can put another shellcode in this exploit.
Why did you a 2011 thread?

mtsmts

chrisk8er - April 20, 2013, 5:29 pm

the shellcode write sos.txt only.
you have to change the shellcode to exploit it. and the video used costum bind shell.
check <http://www.senseofsecurity.com.au/advisories/SOS-10-002>

Code * Shellcode Note:

- * The shellcode writes "pwn-isapi" to "sos.txt" which is created in the current working directory.
- * Most operating systems should be supported by this shellcode. I've used Skylined's method of finding
 - * the base address of kernel32.dll for Windows 7 and modified it so that it will find the base
 - * address of msvcrt.dll instead. I've also added another check so that it will be able to detect
 - * "msvcrt.dll" on Windows Server 2003 (this OS loads msvcrt.dll in 5th position, and before this
 - * DLL string is read, another DLL (RPCRT4.dll) length is verified which matches the length of
 - * msvcrt.dll. So the added check will verify the presents of "m" before proceeding.

Sekret - February 23, 2014, 3:35 am

Didnt get this working either

thegodhello - February 23, 2014, 6:06 am

This doesn't work

sadly :(

I would've used it!

taurus366 - March 8, 2014, 3:11 pm

warning c4530 c++ exception handler used but unwind semantics are not enabled. specify /ehsc
what is this? help me please

run_finder - March 8, 2014, 8:46 pm

I can't seem to get this to work. Any help would be appreciated.

Landchester_Turtle - December 4, 2015, 6:58 am

Thanks for this I'm learning more about the Web everyday on this site

Pluralistic ignorance - December 4, 2015, 12:16 pm

I swear to god all this section has is gravedigs

GOD OF SARADOMIN - December 4, 2015, 3:41 pm

its doesnt work for me rly :/

ren11234 - *October 15, 2019, 7:12 pm*

im trying to do this with the metasploit module, can someone help me out? will tip!