

Buffer overflow in Shell32.dll . Net monitor

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-05/0066.html>

From: David F. Madrid (*idoru_at_VIDEOSOFT.NET.UY*)

Date: 05/30/03

Date: Fri, 30 May 2003 00:51:05 +0200

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Issue

Buffer overflow in Shell32.dll . Net monitor

Tested version

W2000 Server Sp3 Shell32.dll versión 5.0.3502.5436

Vendor status

Microsoft was informed months ago but as they seem to be even slower than me debugging I dediced to publish it .

Descripción

Net monitor is a traffic analysis tool that ships with some versions of Windows .

Besides analyzing traffic you can open capture files (.cap) . If you try to open

a capture file with a long file name (~252 bytes) netmon will crash with an

access violation . Program instruction pointer EIP is overwritten with the file

name converted to unicode , therefore the cause of the crash is a corruption of adjacent variables in the stack . In order to execute code with this vulnerability

you can place your code in a system enviroment variable . That place your code

in an address (~00010040) that can be referenced from our controled EIP converted to unicode .

The crash occurs in this function

```
77E3A294 8B4424 04 MOV EAX,DWORD PTR SS:[ESP+4]
```

```
77E3A298 CD 2B INT 2B
```

```
77E3A29A C2 0400 RETN 4
```

NT-Bugtraq: Buffer overflow in Shell32.dll . Net monitor

After executing int 2B , program seems to change stack and ESP has the value of ~6bf88 . This memory zone is overwritten in the second call to MultiByteToWideChar function in module shell32.dll

```
775C059B FF7424 10 PUSH DWORD PTR SS:[ESP+10] ( Wide buffer size =
260 bytes )
775C059F 66:890E MOV WORD PTR DS:[ESI],CX
775C05A2 8A50 02 MOV DL,BYTE PTR DS:[EAX+2]
775C05A5 80E2 34 AND DL,34
775C05A8 80FA 34 CMP DL,34
775C05AB 0F84 8AA20400 JE SHELL32.7760A83B
775C05B1 56 PUSH ESI (
pointer to Wide buffer )
775C05B2 83C0 0E ADD EAX,0E
775C05B5 6A FF PUSH -1
775C05B7 50 PUSH EAX (
filename )
775C05B8 51 PUSH ECX
775C05B9 51 PUSH ECX
775C05BA FF15 68185977 CALL DWORD PTR DS:[<&KERNEL32.MultiByteToWideChar>]
```

I think the cause is in this call , because when converting to unicode a filename of 252 bytes the wide buffer size should be at least of 504 bytes .

This sencond call to MultiByteToWideChar is made from GetOpenFileNameW , which opens a dialog to choose the file to open and fills a OpenFileName structure with the chosen file name and path . GetOpenFileNameW call completes correctly , the crash occurs a bit after , when executing the 2b interrupt . I ignore what does this interrupt do , I have found in google is reserved for DOS and is equivalent to RET .

Every note or correction will be wellcome cause I am just a student and this is not tough at university :D

Exploit

In the spanish version of this advisory you can find a script to generate the long file name that will crash netmon when open in it

http://nautopia.coolfreepages.com/vulnerabilidades/shell32_getOpenFileNameW.htm

Regards ,

NT-Bugtraq: Buffer overflow in Shell32.dll . Net monitor

David F. Madrid ,
Madrid , Spain

oo
Delivery co-sponsored by TruSecure
oo
FREE 14-DAY TRIAL of New Threat & Vulnerability Notification Service

TruSecure's new IntelliShield(tm) web-based threat and vulnerability service isn't your typical alert service. Supported by TruSecure's vast intelligence resources – including the ICSA Labs – IntelliShield's early warning, analysis, decision support, and threat management tools provide organizations with unmatched intelligence to better protect critical information assets. Experience it for yourself – just click below to begin your FREE, NO OBLIGATION 14-day trial today!

<http://www.trusecure.com/offer/s0074/>

oo