

FW: ITG: buffer overflow & detailed analyses of bug in sens.dll

Source:

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.networking/2004-04/1134.html>

From: Johnny Vogels (*johnnyvogels_at_hotmail.com*)

Date: 04/18/04

Date: 18 Apr 2004 07:32:17 -0700

Haven't heard from this for over 6 months, so I'm posting it here.

It's a very pesky bug, which I encountered frequently with my wifi-card (before I changed the executable)

It would be nice to look at the source of this code...

– Johnny

XXXXXXXXXXXXXXXXXXXXXXXXXXXX

Hello, my name is Brian Murphy and I'm working with the Windows Sustained Engineering team at Microsoft. I have forwarded this issue to the appropriate test engineer for investigation.

Thank you,

Brian Murphy

Windows Sustained Engineering

From: Stefan Schmitt

Sent: Thursday, August 07, 2003 2:14 PM

To: Brian Murphy (Volt)

Subject: AW: ITG: buffer overflow & detailed analyses of bug

microsoft.public.win2000.networking: FW: ITG: buffer overflow & detailed analyses of bug in sens.dll

Please open a bug and assign it appropriately. This may be related to/caused by 38461.

-----Ursprüngliche Nachricht-----

Von: Brian Murphy (Volt)
Gesendet: Thursday, August 07, 2003 2:06 PM
An: Stefan Schmitt
Betreff: RE: ITG: buffer overflow & detailed analyses of bug

Should this be treated as a betabug as well, and a bug opened or is this like the newsgroup issues where we assign to a tester and let them determine if a bug needs to be opened?

From: Stefan Schmitt
Sent: Thu 8/7/2003 1:40 PM
To: Brian Murphy (Volt)
Subject: WG: ITG: buffer overflow & detailed analyses of bug

Can you investigate and find an appropriate owner in the test org?

Thanks,

StefanJ

-----Ursprüngliche Nachricht-----

Von: Miranda Wagner (Kelly Services Inc)
Gesendet: Thursday, August 07, 2003 11:42 AM
An: Stefan Schmitt
Cc: Windows 2000 Service Pack Beta Admin
Betreff: FW: ITG: buffer overflow & detailed analyses of bug

Hi Stefan. Per Trine, she said you were still the right person to handle these issues even though SP4 is now live. Can you reply directly to this customer, johnnyv@MIT.EDU, and cc the w2kspadm alias?

FW: ITG: buffer overflow & detailed analyses of bug in sens.dll

microsoft.public.win2000.networking: FW: ITG: buffer overflow & detailed analyses of bug in sens.dll

Thank you.

Miranda

-----Original Message-----

From: Information Security
Sent: Thursday, August 07, 2003 10:53 AM
To: w2kspadm
Subject: FW: ITG: buffer overflow & detailed analyses of bug

Hello,

Which alias would handle external user bug reports for W2K SP4 ? Thank you.

[THREAD ID:2-9ZUCM]

-----Original Message-----

From: security@microsoft.com
Sent: 7/31/2003 01:44:03 PM
To: "Information Security" <netsec@microsoft.com>
Cc: "Security – Corporate Security Services" <security@microsoft.com>
Subject: ITG: buffer overflow & detailed analyses of bug

Netsec,

For your review.

Thank you,

Trish
Security Service Desk
Redmond, Washington
425.70.34646
M–F, 6 am – 10 pm (PDT)
Security <<http://security/>>

-----Original Message-----

From: Johnny Vogels [mailto:johnnyv@MIT.EDU]
Sent: Thursday, July 31, 2003 8:46 AM
To: Security – Corporate Security Services
Subject: buffer overflow & detailed analyses of bug

Dear Mr/Mrs,

I have found a buffer overflow in the Sens service in windows2000, service pack 4. The fileversion of the file, sens.dll, is

FW: ITG: buffer overflow & detailed analyses of bug in sens.dll

microsoft.public.win2000.networking: FW: ITG: buffer overflow & detailed analyses of bug in sens.dll
5.0.2195.6627.

xxxxxxxxxxxxx reproduction xxxxxxxxxxxxxxxxxxxxxxx

Requirements:

- > *windows2000, sp4, internet explorer 6.0.2800.1106*
- > *a removable ethernet device such as lan card, or preferrably, a removable wifi device.*
- > *a working internet connection*
- > *optional: windbg 6.0.0007.0 (for seeing what is happening in the sens service)*

The reproduction is a bit involved, and can take up to half an hour.
Therefore, windbg is used to see the progress being made.

step 1

attach windbg to the svchost which runs the sens service

step 2

monitor memory adress 76188160 with windbg and onward

step 3

set a breakpoint in windbg at

761833e5: EvaluateLanConnectivity

note 1)

for steps 4 to ...: windbg will hit the breakpoint set in step 3 during
these steps. Press F5 (Go) to continue each time this happens.

note 2) MAKE SURE THAT EVALUATELANCONNECTIVITY GETS CALLED BETWEEN
EACH STEP BY TRYING TO GET A PAGE IN INTERNET EXPLORER.

step 4

connect the lan device

step 5

establish a connection (by connecting the cable, or establish a wifi connection)

step 6

stop the connection

step 7

Stop the device and remove it from the computer.

Especially after this step one has to make sure that `evaluatelanconnectivity` get called by using internet explorer. With a lan card It might take up to two minutes before i.e. calls `evaluatelanconnectivity`, but it seems instantaneous for wifi cards. This calls `PurgeStaleInterfaces`, which is required.

repeat step 4

Note: during each cycle, the counter at `0x76188244` gets increased by 1, and a later element in the `IfState` interface state table at address `0x76188160` gets called, until it overflows over into `0x76188228`

Note, that if `WANState` is not 0, the overflow does not happen, because `HasIfStateChanged` then thinks element 5, which does not exist, is already being used, and then uses the first element of the table. In my configuration `WANState` is 0.

I'm not whether `EvaluateWanConnectivity` gets called using a normal lan card. One might need a wifi card for this. I'm also not sure under exactly which conditions it calls the routine pointed to by

microsoft.public.win2000.networking: FW: ITG: buffer overflow & detailed analyses of bug in sens.dll
RasEnumConnection. But if it does, it results in a protection fault.

xxxxxxxxxxxxx end of reproduction xxxxxxxxxxxxxxxx

xxxxxxxxxxxxx detailed analyses of the bug xxxxxxxxxxxxxxxxxxxxxxxx

This bug was localized using windbg 6.0.0007.0, attaching it to the particular svchost.exe instance which runs the sens service.

The buffer in question is the IfState interface state table at address 0x76188160 maintained by HasIfStateChanged and PurgeStaleInterfaces, both called by EvaluateLanConnectivity.

This table is has five elements, no# 0 to 4, consisting of 10 words each.

HasIfStateChanged also maintains a counter at 0x76188244, which keeps number of the last used element. This number is checked to never exceed 4. This number is used if a new interface is to be added: If the next element is not full, which is determined by the first word of the next element, it will be used. The problem is that this next element might be element number 5, A CONDITION WHICH IS NOT CHECKED FOR. In this case the 10 words from 0x76188228 to 0x7618824F are overwritten. This range of addresses contains the following variables:

0x76188228: WANState

0x7618822C: IsRasInstalled

0x76188230: LastWANTime

0x76188234: RasEnumConnection

0x76188238: ???

0x7618823C: ???

0x76188240: FailureHook

microsoft.public.win2000.networking: FW: ITG: buffer overflow & detailed analyses of bug in sens.dll

0x76188244: counter referred to above !!!

0x76188248: ???

0x7618824C: ???

Because RasEnumConnection is a pointer to a function, called for example at address 0x761831ae in EvaluateWanConnectivity, this eventually results in a protection fault.

XXXXXXXXXXXXXXXXXX end detailed analyses of the bug
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXX security analyses XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

The address being called in EvaluateWanConnectivity is word 4 (first element 0) of an interface table. It seems hard to exploit this.

XXXXXXXXXXXXXXXXXX security analyses XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXX further comments XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

For this bug to occur, one has to reach the end of the ifState table, which has five elements. This can be accomplished by removing an ethernet device five times, and invoking internet explorer while the device is removed. This has to be done at least five times. This made this bug very hard to track down. This bug will eventually be encountered eventually, and take down the svchost.exe which is running it. This requires a reboot of the computer to recover. I therefore strongly recommend fixing it.

