

Re: [Full-Disclosure] Re: Serious flaws in bluetooth security lead to disclosure of personal data

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-11/0777.html>

From: Pentest Security Advisories (*alerts_at_pentest.co.uk*)

Date: 11/15/03

To: nosp <nosp@xades.com>

Date: Sat, 15 Nov 2003 13:40:14 +0000

On Fri, Nov 14, 2003 at 04:05:36PM +0000, nosp wrote:

> *On Fri, 2003-11-14 at 10:21, Pentest Security Advisories wrote:*
> *[...]*
> > *No, you didn't misread - The T610, whilst still vulnerable to some*
> > *attacks, does provide more protection*
> > *of OBEX profiles. In this respect, it's better than the other phones /*
> > *devices we've tested.*
> >
> > *On the particular T610 that was tested, we found that whilst it was*
> > *possible to upload files to the phone we could not download files from it.*
>
> *It is very possible (and easy) to download (very) sensitive files from a*
> *T610 as long as the MAC is known; no pairing necessary. Firmware rev*
> *R3C002. Files include calendar and phonebook.*
>

I retested the T610 and got the following,

Service Name: Dial-up Networking

Channel: 1

State: Closed.

Service Name: Voice gateway

Channel: 3

State: Closed.

Service Name: Serial Port 1

Channel: 4

State: Closed.

Service Name: Serial Port 2

Channel: 5

State: Closed.

Full-Disclosure: Re: [Full-Disclosure] Re: Serious flaws in bluetooth security lead to disclosure of personal data

Service Name: OBEX Object Push

Channel: 10

State: Open.

GET telecom/pb.vcf

Returns Unauthorised

GET telecom/cal.vcs

Returns Unauthorised

GET telecom/pb/0.vcf

Returns Unauthorised

Service Name: IrMC Synchronization

Channel: 11

State: Closed.

Service Name: HF Voice gateway

Channel: 6

State: Closed.

Service Name: OBEX Basic Imaging

Channel: 15

State: Open.

GET telecom/pb.vcf

Returns Unauthorised

GET telecom/cal.vcs

Returns Unauthorised

GET telecom/pb/0.vcf

Returns Unauthorised

Service Name: OBEX File Transfer

Channel: 7

State: Closed.

The firmware version is: R1L013

It appears that this firmware version is not vulnerable. A quick google shows that it may be due to other problems in the firmware.

Tim.

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>