Bip - Bug #432

authenticated bip users could stop bip daemon

2015-01-15 04:56 - Pierre-Louis Bonicoli

Status:	In Progress	**Start date:**	2015-01-15
Priority:	Normal	**Due date:**	
Assignee:	Pierre-Louis Bonicoli	**% Done:**	80%
Category:		**Estimated time:**	0:00 hour
Target version:	0.9.0		
Patch Available:	Yes	**Branch:**	
Found in Versions:		**Security:**	Yes
Confirmed:	Yes	**Help Needed:**	

Description

Fran found that these commands allow an authenticated bip user to stop bip daemon:

```
{ echo PASS bipnick:mysecretpassword:freenode; echo NICK Pilou; echo USER Pilou 0 Pilou :blah; sle
ep 2; } | telnet 127.0.0.1 7778 | read
```

```
15-01-2015 04:26:44 DEBUG: Trying to accept new client on 0
15-01-2015 04:26:44 DEBUG: New client on socket 41 !
15-01-2015 04:26:44 DEBUG: fd:41 Connection established !
15-01-2015 04:26:44 DEBUG: "PASS bipnick:mysecretpassword:freenode"
15-01-2015 04:26:44 DEBUG: "NICK Pilou"
15-01-2015 04:26:44 DEBUG: "USER Pilou 0 Pilou :blah"
15-01-2015 04:26:44 DEBUG: Connection close asked. FD:41
15-01-2015 04:26:44 DEBUG: A client connected
15-01-2015 04:26:44 FATAL: select(): Bad file descriptor
```

History

#1 - 2015-01-15 05:02 - Pierre-Louis Bonicoli

- Subject changed from Fatal to authenticated bip users could stop bip daemon

- Description updated

#2 - 2015-01-16 07:28 - Pierre-Louis Bonicoli

- File patch added

- Status changed from New to In Progress

- Assignee set to Pierre-Louis Bonicoli

This bug is the plaintext counterpart of #261 (which was related to SSL connections).

The attached patch fixes the problem for plaintext connections. I need to test behavior with SSL connections.

#3 - 2015-08-29 03:06 - Pierre-Louis Bonicoli

- Target version set to 0.9.0

- % Done changed from 0 to 80

- Patch Available set to Yes

There is no problem when client_side_ssl is enabled.

Tested with these commands:

```
$ socat -s TCP4-LISTEN:8000 OPENSSL:127.0.0.1:7778,verify=0 &
$ { echo PASS bipnick:mysecretpassword:freenode; echo NICK Pilou; echo USER Pilou 0 Pilou :blah; sleep 2; } |
telnet 127.0.0.1 8000 | read
```

Files

patch	3.8 KB	2015-01-16	Pierre-Louis Bonicoli