Bip - Bug #269

buffer overflow when number of open file descriptors >= FD_SETSIZE

2012-01-07 11:28 - Pierre-Louis Bonicoli

Status:	Resolved	**Start date:**	2012-01-07
Priority:	Urgent	**Due date:**	
Assignee:	Pierre-Louis Bonicoli	**% Done:**	50%
Category:		**Estimated time:**	0:00 hour
Target version:			
Patch Available:	Yes	**Branch:**	
Found in Versions:	0.7.0 0.8.8	**Security:**	Yes
Confirmed:	Yes	**Help Needed:**	No

Description

Reported by Julien Tinnes, thanks to him!

Bip doesn't check if fd is equal or larger than FD_SETSIZE.

From select man page:

> Executing FD_CLR() or FD_SET() with a value of fd that is negative or is equal to or larger than FD_SETSIZE will result in undefined behavior.

History

#1 - 2012-01-07 11:45 - Pierre-Louis Bonicoli

- File 0001-Buffer-Overflow-check-against-the-implicit-size-of-s.patch added

- Subject changed from buffer overflow when number of open file descriptors >= 1024 to buffer overflow when number of open file descriptors >= FD_SETSIZE

- Description updated

Patch added.

#2 - 2012-01-07 16:07 - Pierre-Louis Bonicoli

As stated by Nohar, server sockets must be checked too !

#3 - 2012-01-24 00:14 - Pierre-Louis Bonicoli

- Status changed from In Progress to Resolved

- Found in Versions changed from 0.8.2 0.8.8 to 0.7.0 0.8.8

Fixed 222a33cb84a2e52ad55a88900b7895bf9dd0262c

#4 - 2012-01-24 00:14 - Pierre-Louis Bonicoli

- Private changed from Yes to No

Files

0001-Buffer-Overflow-check-against-the-implicit-size-of-s.patch	1.64 KB	2012-01-07	Pierre-Louis Bonicoli