Libprelude - Bug #54

Segmentation Fault if the client profile is not properly set

02/21/2005 10:11 AM - Sebastien Tricaud

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Yoann VANDOORSELAERE	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Resolution:	invalid		

Description

When using the function prelude_connection_connect(), if the prelude client profile is not properly initialized before, that will result in a segfault.

Try to put NULL as the third parameter to this function.

I know it's bad and the prelude client profile MUST be initialized and we should check the return value to see if there was something wrong or not. However, IMHO libprelude should check the client profile before calling "do_connect(conn, profile);" Or maybe do it in prelude_client_profile_get_credentials().

This is the backtrace I've got :

```
Program received signal SIGSEGV, Segmentation fault.
[Switching to Thread -1210818432 (LWP 10744)]
prelude_client_profile_get_credentials (cp=0x0, credentials=0x8067dc8) at prelude-client-profile.c
:428
428             if ( cp->credentials ) {
(gdb) bt
#0  prelude_client_profile_get_credentials (cp=0x0, credentials=0x8067dc8) at prelude-client-profi
le.c:428
#1  0xb7f92019 in tls_auth_connection (cp=0x0, io=0x8067dc8, crypt=1, analyzerid=0x0) at tls-auth.
c:150
#2  0xb7f958fd in handle_authentication (cnx=0x8066fb8, cp=0x0, crypt=0) at prelude-connection.c:2
36
#3  0xb7f959c6 in start_inet_connection (cnx=0x8066fb8, profile=0x0) at prelude-connection.c:263
#4  0xb7f95b5f in do_connect (cnx=0x8066fb8, profile=0x0) at prelude-connection.c:319
#5  0xb7f961ce in prelude_connection_connect (conn=0x8066fb8, profile=0x0, capability=3) at prelud
e-connection.c:559
#6  0x08048cd3 in main ()
```

Now I'll use the prelude_client_profile_new() function to avoid this smile.png

History

#1 - 02/21/2005 10:41 AM - Yoann VANDOORSELAERE

- Status changed from New to Closed

- Resolution set to invalid

This expected. You are required to provide a profile object for connecting to the peer.

#2 - 04/29/2009 12:26 PM - Yoann VANDOORSELAERE

- Project changed from PRELUDE SIEM to Libprelude

- Category deleted (1)