Subject: Core/SSL crashes at exit on Linux.
Posted by Oblivion on Fri, 02 Feb 2018 12:06:02 GMT
View Forum Message <> Reply to Message

Hello,

SSL 1.1.0, crashes on cleanup (always).

(InitExit.cpp, line 90):

sk_SSL_COMP_free(pCOMP); // According to gdb, pCOMP seems to be a a valid pointer but app crashes after this line.
// Commenting out this line prevents crashes, but I'm not sure if it leaks or not. (U++'s allocators don't complain)

It crashes after this line, not in it, so a double freeing might be happening. I'm not familiar with low level code of OpenSSL but it says:

https://www.openssl.org/docs/man1.1.0/ssl/SSL_COMP_add_compr ession_method.html
Quote:
In versions of OpenSSL prior to 1.1.0 SSL_COMP_free_compression_methods() freed the internal table of compression methods that were built internally, and possibly augmented by adding SSL_COMP_add_compression_method(). However this is now unnecessary from version 1.1.0. No explicit initialisation or de-initialisation is necessary. See OPENSSL_init_crypto and OPENSSL_init_ssl. From OpenSSL 1.1.0 calling this function does nothing.

Best regards,
Oblivion

Subject: Re: Core/SSL crashes at exit on Linux.
Posted by mirek on Tue, 06 Feb 2018 10:01:28 GMT
View Forum Message <> Reply to Message

Hopefully fixed (with #ifdef). Please check.

I was testing in Debian 9 - in the process, I have noticed another problem with SslRealloc - SSL there was calling that with NULL ptr and non-zero size. That should be now fixed as well...

Subject: Re: Core/SSL crashes at exit on Linux.
Posted by Oblivion on Tue, 06 Feb 2018 12:07:55 GMT
View Forum Message <> Reply to Message

Hello Mirek,

Now it seems to work fine. No crashes. Thanks!

Best regards,
Oblivion.