strongSwan - Bug #3045

Build failure with OpenSSL 1.1.1 without API compatibility layer

07.05.2019 06:57 - Lucian Cristian

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	build		
Target version:	5.8.0		
Affected version:	5.7.2	**Resolution:**	Fixed

Description

compiling openssl module fails to load with

```
daemon.info : 00[LIB] plugin 'openssl' failed to load: Error relocating /usr/lib/ipsec/plugins/lib
strongswan-openssl.so: X509_get_notAfter: symbol not found
```

openssl says X509_get_notBefore() and X509_get_notAfter() were deprecated in OpenSSL 1.1.0

a fix

```
--- a/src/libstrongswan/plugins/openssl/openssl_x509.c  2019-04-30 15:30:59.590212295 +0300
+++ b/src/libstrongswan/plugins/openssl/openssl_x509.c  2019-04-30 15:31:32.158213669 +0300
@@ -1137,8 +1137,8 @@
                 return FALSE;
         }

-       this->notBefore = openssl_asn1_to_time(X509_get_notBefore(this->x509));
-       this->notAfter = openssl_asn1_to_time(X509_get_notAfter(this->x509));
+       this->notBefore = openssl_asn1_to_time(X509_get0_notBefore(this->x509));
+       this->notAfter = openssl_asn1_to_time(X509_get0_notAfter(this->x509));

         /* while X509_ALGOR_cmp() is declared in the headers of older OpenSSL
          * versions, at least on Ubuntu 14.04 it is not actually defined */
```

but maybe **openssl_asn1_to_time** should also be changed to accept a const parameter. Compatibility defines for OpenSSL 1.0.2 would be a good idea as well.

Associated revisions

Revision a4abb263 - 08.05.2019 14:28 - Tobias Brunner

openssl: Fix build with OpenSSL 1.1.1 without compatibility layer

If OpenSSL is built with --api, defines for deprecated functions in
OpenSSL's header files are not visible anymore.

Fixes #3045.

History

#1 - 07.05.2019 15:07 - Tobias Brunner

- Status changed from New to Feedback

Thanks for the report.

If OPENSSL_API_COMPAT is defined (and lower than 1.1.0), the openssl/x509.h header has defines for the deprecated functions (it actually maps them to X509_getm_notBefore|After, whose non-const interface probably matches the previous functions more closely).

So this actually works fine if OpenSSL is built with compatibility layer, which is the case by default (i.e. if no API level is explicitly configured). For example, see our Travis CI build that currently uses OpenSSL 1.1.1b and does not specify an API level.

> but maybe openssl_asn1_to_time should also be changed to accept a const parameter

It already does (source:src/libstrongswan/plugins/openssl/openssl_util.h#L136).

I pushed some commits to the *travis-openssl-api* branch, which also disable OpenSSL's compat layer.

#2 - 07.05.2019 15:08 - Tobias Brunner

- Tracker changed from Issue to Bug

- Subject changed from OpenSSL 1.1.1 to Build failure with OpenSSL 1.1.1 without API compatibility layer

- Assignee set to Tobias Brunner

- Target version set to 5.8.0

- Resolution set to Fixed

#3 - 08.05.2019 14:59 - Tobias Brunner

- Status changed from Feedback to Closed

Fix is now in master.