strongSwan - Issue #2560

Duplicate CA cert requests sent

23.02.2018 12:06 - Luka Logar

Status:	Feedback		
Priority:	Normal		
Assignee:			
Category:			
Affected version:	5.6.2	**Resolution:**	

Description

We are using certificates stored on smartcards (both user & CA certs). Some hosts also have (same) CA certificates stored localy in x509ca directory. In such cases strongSwan sends duplicate cert requests for the (same) CA certificates that are stored both on card and in x509ca directory. I think duplicate certs should be filtered out (as is currently done for example in vici plugin)...

History

#1 - 23.02.2018 14:42 - Tobias Brunner

- Status changed from New to Feedback

> I think duplicate certs should be filtered out (as is currently done for example in vici plugin)...

There is currently no code that filters duplicate CA certificates. All CA certificates found in any of the credential sets will be considered when sending certificate requests (unless remote CAs are specifically configured in the config). Not sure if it's worth it to complicate that as it is probably not that common to have the same CA certificate in multiple locations.

#2 - 23.02.2018 15:00 - Luka Logar

It looked to me that *enum_certs()* in *vici_query.c* did exactly that - adds only unique certs to the linked list (ignoring duplicates)? Otherwise, I agree it's just cosmetics.

#3 - 23.02.2018 15:07 - Tobias Brunner

> It looked to me that *enum_certs()* in *vici_query.c* did exactly that - adds only unique certs to the linked list (ignoring duplicates)?

It does, but that's totally unrelated to the certificate requests.

#4 - 23.02.2018 16:53 - Luka Logar

> It does, but that's totally unrelated to the certificate requests.

I know that, I just refered to your comment that there is no code that filters duplicate CA certificates. The few lines of code in *enum_certs()* which filter duplicate certificates before they are sent to the swanctl --list-certs, could also be used in the *build_certreqs()* function...

Anyway you can close this issue, If you think it's not worh fixing...

#5 - 28.02.2018 10:54 - Tobias Brunner

> > It does, but that's totally unrelated to the certificate requests.
>
> I know that, I just refered to your comment that there is no code that filters duplicate CA certificates. The few lines of code in *enum_certs()* which filter duplicate certificates before they are sent to the swanctl --list-certs, could also be used in the *build_certreqs()* function...

That code is quite inefficient, though, if there are lots of CAs, as the encoding of every enumerated CA certificate is compared to all previous ones (the Android app, for instance, loads all CAs on the system by default, and the NM plugin can do the same). Something like the code in the

2560-certreq-dups branch might be a better approach (it has a bit more memory overhead, but it is computationally more efficient as the keyid has to be calculated anyway and the chunk hashes for these 20 bytes can be calculated quickly). Still not sure if it is really worth it, though.