strongSwan - Bug #3667

loadtest cert padding error on serial for LANCOM gateway

07.01.2021 13:23 - olaf Rottler

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.9.2		
Affected version:	5.8.0	**Resolution:**	Fixed

Description

Hallo,

using the loadtest with IKEv2 against cisco asa without problems.
First Time against LANCOM this on fails on strongswan client cert with cert padding error on serial number;

cert with serial number: 000001, subject name: CN=9999999999920001, issuer_name:
CN=CA-DATEV-loadtest,OU=P354,L=Nuernberg,C=DE.

Fortigate fails too on the cert, but without any hint.
You have any idea ?

Both vendors ask for the sending the client cert, therefore I failed too trying to generate a simular cert from scratch failed with public key

```
pki --gen --size 3072 > /etc/ipsec.d/myKey9999999999920001.der
 pki --req --in /etc/ipsec.d/myKey9999999999920001.der --dn "CN=9999999999920001" --out /etc/ipsec
.d/aacerts/9999999999920001requ.der
  pki --issue --type rsa --in /etc/ipsec.d/aacerts/rottkey9999999999920001requ.der --cakey /etc/ip
sec.d/private/load.der --cacert /etc/ipsec.d/cacerts/caCert.der  --dn "CN==9999999999920001" --out
form pem
building CRED_PRIVATE_KEY - RSA failed, tried 7 builders
parsing public key failed
```

Would this indentical to the loadtest ?
How can I get this (I think I did configure openssl too, otherwise loadtest would not work).
Or could you just send me any root, key and client cert for passing it to both vendors ?

Greetings
Olaf

Associated revisions

Revision bd9b50dc - 18.01.2021 17:44 - Tobias Brunner

load-tester: Correctly encode serial of generated client certificates

The previous approach would lead to additional zero prefixes in the
encoding of the serial (which is a positive integer, not an arbitrary
blob).

Fixes #3667.

History

#1 - 07.01.2021 13:57 - Tobias Brunner

- Category set to configuration

- Status changed from New to Feedback

First Time against LANCOM this on fails on strongswan client cert with cert padding error on serial number;

Sorry, I don't understand what that means.

> pki --gen --size 3072 > /etc/ipsec.d/myKey9999999999920001.der
> pki --req --in /etc/ipsec.d/myKey9999999999920001.der --dn "CN=9999999999920001" --out /etc/ipsec.d/aacerts/9999999999920001requ.der
> pki --issue --type rsa --in /etc/ipsec.d/aacerts/rottkey9999999999920001requ.der --cakey /etc/ipsec.d/private/load.der --cacert /etc/ipsec.d/cacerts/caCert.der --dn "CN==9999999999920001" --outform pem

If you want to use a PKCS#10 certificate request as input for --issue, you have to use --type pkcs10 and not rsa. But that seems unecessary if you pass --dn to --issue too (note that there is a typo).

> Would this indentical to the loadtest ?

No, why should that be identtical?

> Or could you just send me any root, key and client cert for passing it to both vendors ?

The default CA key and certificate can be found here: source:src/libcharon/plugins/load_tester/load_tester_creds.c

Client certificates are created/issued on the fly (same source file, note that the private key is the same for these and the CA).

#2 - 07.01.2021 17:55 - olaf Rottler

Ah sure, sorry, I get the the cert now with pkcs. Thanks a lot and a Happy New Year !
Just for understanding, I only guessed you would use the same pki library from load_tester_creds.c and the pki command line, so the result would be simular regarding "padding" the remote gateway complained about.
Should be easy to verify that with a single connection try, but now I run in charon has quit: integrity test of libstrongswan failed () on my old but updated debian.
Will prepare a new debian server and try nect week again.

#3 - 07.01.2021 18:08 - Tobias Brunner

> Just for understanding, I only guessed you would use the same pki library from load_tester_creds.c and the pki command line, so the result would be simular regarding "padding" the remote gateway complained about.

What do you mean with "padding" in this context?

> Should be easy to verify that with a single connection try, but now I run in charon has quit: integrity test of libstrongswan failed () on my old but updated debian.

Did you mix Debian packages with builds from source?

#4 - 07.01.2021 18:45 - olaf Rottler

But you are sure, that cert with serial number: *0000*01, subject name: CN=9999999999920001, issuer_name: ... is RFC conform ?
May bee the integer should be encoded with the minimal possible form https://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf.
I know the loadtest is inteded for strongswan itself, but would be nice to use it against other vendors too.

#5 - 07.01.2021 19:28 - olaf Rottler

Sorry, Padding is an error (debug) message from LANCOM Firmware, I can only guess it is not related to the cert padding overall, instead may be only to the leading zeros because the serial number is explicit mentioned too in this debug event.

I didn't planned to mix the packages, but from the long history I'm never sure, will do a new build together with the new server.

#6 - 08.01.2021 10:09 - Tobias Brunner

- Tracker changed from Issue to Bug

- Category changed from configuration to libcharon

- Target version set to 5.9.2

> But you are sure, that cert with serial number: *0000*01, subject name: CN=9999999999920001, issuer_name: ... is RFC conform ?

Ah, now I see what you mean. Yeah, that's not correct. The serial must be a positive integer that's encoded in the least number of bytes (there could

be a zero prefix, though, if the number would otherwise be negative). However, the load-tester plugin currently encodes a complete 32-bit unsigned integer directly. So that will lead to this padding with additional zero bytes. I pushed a fix for that to the *3667-load-tester-serial* branch. Let me know if that works for you.

#7 - 13.01.2021 14:43 - olaf Rottler

Gereat, it works for fortigate immed. and for LANCOM up to the next error
"-Remote-ID (DIGITAL_SIGNATURE, ID_NONE:ID_NONE): Empty config HASH_ALGORITHMS"
have to check with lancom, it's funny how different all the vendors behave ...
On loadtester I have constant
issuer_key = /etc/ipsec.d/private/load.der
digest = sha256
:::
proposal = aes256gcm16-prfsha1-modp2048
esp = aes256-sha256-modp2048

#8 - 13.01.2021 15:42 - Tobias Brunner

> and for LANCOM up to the next error
> "-Remote-ID (DIGITAL_SIGNATURE, ID_NONE:ID_NONE): Empty config HASH_ALGORITHMS"

Is that actually concerning the certificate? Might be something else (e.g. related to the hash algorithms negotiated for RFC 7427 signature authentication). But yeah, you better ask LANCOM what exactly it means.

#9 - 18.01.2021 17:46 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to Fixed

#10 - 22.01.2021 17:33 - olaf Rottler

Yes, that was only some stupid configuration result of there GUI. A more experienced colleg could fix it on cli level. It works now as expected. Thanks a lot for the fast fix !!!