strongSwan - Bug #2509

Certificates with serial numbers with MSB set, can not be revoked (when using openssl plugin)

08.01.2018 00:36 - Luka Logar

Status:	Closed	**Start date:**	08.01.2018
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libstrongswan		
Target version:	5.6.2		
Affected version:	5.6.1	**Resolution:**	Fixed

Description

I am using IKEv2 certificate based strongSwan 5.6.1 (with openssl plugin) site-to-site VPN. I've found out, that some revoked certificates can still be used as valid even though a valid CRL is present and loaded by the revocation plugin. Here's what I think is happening:

The certificates in question have serial numbers with MSB set. As such, their serial numbers are ASN1 DER encoded with a leading 0x00 byte.

It seems that openssl ASN1_INTEGER type internaly stores integers with MSB set without leading 0x00 byte (negative numbers are marked by type V_ASN1_NEG_INTEGER).
As openssl plugin constructs serialNumber chunk by calling openssl_asn1_str2chunk(X509_get_serialNumber(this->x509)), the chunk is also created without leading 0x00 byte (if the serial number has MSB set).
This leads to revocation plugin failing to find this serial number in the list of revoked serial numbers (chunk_equals() function is used for comparison) and the revoked certificate is marked as valid...

Affected are Strongswan v5.6.1 and openssl 1.0.2n (but probably other versions too)

The attached patch fixes this by prepending a 0x00 byte (if necessary) to the serial number...

Associated revisions

Revision 432358cf - 31.01.2018 10:50 - Tobias Brunner

revocation: Skip any zero bytes when comparing serials in CRLs

Depending on the plugins that eventually parse the certificate and CRL, serials with MSB set (i.e. negative numbers that have a zero byte prefixed when encoded as ASN.1 INTEGER) might have (x509 plugin) or not have (openssl plugin) a zero byte prefix when returned by get_serial() or enumerated from the CRL. Strip them before doing the comparison or revocation checking might fail if not both credentials are parsed by the same plugin (which should be rare and only happen if parsing of either cert or CRL fails with one of the plugins and there is a fallback to the implementation provided by the other plugin).

Fixes #2509.

History

#1 - 09.01.2018 15:01 - Andreas Steffen

- Status changed from New to Feedback

How does openssl 1.0.2n treat serial numbers of revoked certificates in CRLs and how does openssl 1.0.2n comparison of serial numbers in "openssl verify -crl_check"?

#2 - 09.01.2018 17:42 - Luka Logar

I guess openssl is calling ASN1_INTEGER_cmp() to compare serial numbers. But in my case it was irrelevant, as it seems that revocation plugin was using *x509* plugin to parse the crl. I have just noticed that I had both *x509* and *openssl* plugins loaded. If I disable the *x509* plugin (I can't remember why did I enable it in the first place) then *openssl* plugin is used both for certificate decoding and crl decoding/verifying and all is well.

So to sum it up. If the certificate decoding is done by *openssl* and *crl* decoding/verifying is done by *x509* plugin, only then certificate status checking fails. However this is, at least in my case, default behaviour if both plugins are loaded (I should also mention I didn't mess with plugin priorities), so I guess it should nonetheless be fixed...

#3 - 24.01.2018 14:55 - Tobias Brunner

- Target version set to 5.6.2

> So to sum it up. If the certificate decoding is done by *openssl* and *crl* decoding/verifying is done by *x509* plugin, only then certificate status checking fails.

Yeah, the *x509* plugin returns the serials (from cert and CRL) as ASN.1 integer data objects with 0 prefix and the *openssl* plugin returns them without. So when cert and CRL are not parsed by the same plugin the revocation plugin won't find a match.

> However this is, at least in my case, default behaviour if both plugins are loaded (I should also mention I didn't mess with plugin priorities)

This is a bit strange. Because parsing of both cert and CRL should usually be handled by the plugin that is loaded first (at least that's the case in my tests). The only situation where that's not the case is if the first parser for either the cert or CRL fails for some reason and there is a fallback to the other implementation. Could you send me the test certificates/CRLs you used, maybe we can determine what exactly happened.

> so I guess it should nonetheless be fixed...

Agreed, maybe we could use something like the patch in the *2509-revocation-serials* branch. Then it doesn't matter how the serials are returned or which plugin parses the cert and which the CRL (I think your patch does not fix the case where the CRL is parsed by the *openssl* plugin and the cert by the *x509* plugin). We also do this in for other use cases (e.g. when printing certs and CRLs).

#4 - 25.01.2018 12:24 - Luka Logar

With my strongSwan setup *x509* plugin was loaded first and *openssl* second. CRL loading/parsing follows this order. However for cert loading/parsing *openssl* plugin is used first. I believe this is due to the *x509* plugin cert-loading functions depending on PUBKEY/ANY_KEY which (in my case) *openssl* plugin provides, whereas *x509* crl-loading functions have no such dependencies.

Btw. your *2509-revocation-serials* patch is working fine.

#5 - 25.01.2018 15:47 - Tobias Brunner

> With my strongSwan setup *x509* plugin was loaded first and *openssl* second.

Yes, that's the default.

> However for cert loading/parsing *openssl* plugin is used first. I believe this is due to the *x509* plugin cert-loading functions depending on PUBKEY/ANY_KEY which (in my case) *openssl* plugin provides, whereas *x509* crl-loading functions have no such dependencies.

That shouldn't matter (unless you use an old strongSwan version). The plugin loader will load the dependencies provided by the *openssl* plugin, followed by the cert loader of the *x509* plugin before continuing with the rest of the features provided by the *openssl* plugin. You can check if you increase the log level for *lib* to 3, then you see which plugin features are loaded in which order. For instance, if I load the plugins x509 pkcs1 pem openssl revocation with the pki tool I get this (the *openssl* cert and CRL loader are loaded as dependencies of the features provided by the *pem* plugin):

Plugin loading...Plugin loading...

```
plugin 'x509': loaded successfully
plugin 'pkcs1': loaded successfully
plugin 'pem': loaded successfully
plugin 'openssl': loaded successfully
plugin 'revocation': loaded successfully
loading feature CERT_ENCODE:X509 in plugin 'x509'
  loading feature HASHER:HASH_SHA1 in plugin 'openssl'
loading feature CERT_DECODE:X509 in plugin 'x509'
  loading feature PUBKEY:ANY in plugin 'pkcs1'
    loading feature PUBKEY:RSA in plugin 'pkcs1'
    loading feature PUBKEY:RSA in plugin 'pem'
      loop detected while loading PUBKEY:RSA in plugin 'pem'
      loading feature PUBKEY:RSA in plugin 'openssl'
    loading feature PUBKEY:ECDSA in plugin 'pem'
      loop detected while loading PUBKEY:ECDSA in plugin 'pem'
      loading feature PUBKEY:ECDSA in plugin 'openssl'
    loading feature PUBKEY:ED25519 in plugin 'pem'
feature PUBKEY:ED25519 in plugin 'pem' has unmet dependency: PUBKEY:ED25519
    feature PUBKEY:ANY in plugin 'pkcs1' has unmet soft dependency: PUBKEY:ED25519
```

```
    feature PUBKEY:ANY in plugin 'pkcs1' has unmet soft dependency: PUBKEY:ED448
    loading feature PUBKEY:BLISS in plugin 'pem'
feature PUBKEY:BLISS in plugin 'pem' has unmet dependency: PUBKEY:BLISS
    feature PUBKEY:ANY in plugin 'pkcs1' has unmet soft dependency: PUBKEY:BLISS
    loading feature PUBKEY:DSA in plugin 'pem'
feature PUBKEY:DSA in plugin 'pem' has unmet dependency: PUBKEY:DSA
    feature PUBKEY:ANY in plugin 'pkcs1' has unmet soft dependency: PUBKEY:DSA
  loading feature PUBKEY:ANY in plugin 'pem'
    loop detected while loading PUBKEY:ANY in plugin 'pem'
    loading feature PUBKEY:ANY in plugin 'openssl'
loading feature CERT_ENCODE:X509_AC in plugin 'x509'
loading feature CERT_DECODE:X509_AC in plugin 'x509'
loading feature CERT_ENCODE:X509_CRL in plugin 'x509'
loading feature CERT_DECODE:X509_CRL in plugin 'x509'
loading feature CERT_ENCODE:OCSP_REQUEST in plugin 'x509'
  loading feature RNG:RNG_WEAK in plugin 'openssl'
  loading feature RNG:RNG_STRONG in plugin 'openssl'
loading feature CERT_DECODE:OCSP_RESPONSE in plugin 'x509'
loading feature CERT_ENCODE:PKCS10_REQUEST in plugin 'x509'
loading feature CERT_DECODE:PKCS10_REQUEST in plugin 'x509'
loading feature PRIVKEY:ANY in plugin 'pkcs1'
  loading feature PRIVKEY:RSA in plugin 'pkcs1'
  loading feature PRIVKEY:RSA in plugin 'pem'
    loop detected while loading PRIVKEY:RSA in plugin 'pem'
    loading feature PRIVKEY:RSA in plugin 'openssl'
    loading feature HASHER:HASH_MD5 in plugin 'openssl'
  loading feature PRIVKEY:ECDSA in plugin 'pem'
    loop detected while loading PRIVKEY:ECDSA in plugin 'pem'
    loading feature PRIVKEY:ECDSA in plugin 'openssl'
loading feature PRIVKEY:ANY in plugin 'pem'
  loop detected while loading PRIVKEY:ANY in plugin 'pem'
  loading feature PRIVKEY:ANY in plugin 'openssl'
  loading feature PRIVKEY:ANY in plugin 'openssl'
loading feature PRIVKEY:DSA in plugin 'pem'
feature PRIVKEY:DSA in plugin 'pem' has unmet dependency: PRIVKEY:DSA
loading feature PRIVKEY:BLISS in plugin 'pem'
feature PRIVKEY:BLISS in plugin 'pem' has unmet dependency: PRIVKEY:BLISS
loading feature PRIVKEY:ED25519 in plugin 'pem'
feature PRIVKEY:ED25519 in plugin 'pem' has unmet dependency: PRIVKEY:ED25519
loading feature CERT_DECODE:ANY in plugin 'pem'
  loading feature CERT_DECODE:X509 in plugin 'pem'
    loop detected while loading CERT_DECODE:X509 in plugin 'pem'
    loading feature CERT_DECODE:X509 in plugin 'openssl'
      feature CERT_DECODE:X509 in plugin 'openssl' has unmet soft dependency: PUBKEY:DSA
  loading feature CERT_DECODE:PGP in plugin 'pem'
feature CERT_DECODE:PGP in plugin 'pem' has unmet dependency: CERT_DECODE:PGP
  feature CERT_DECODE:ANY in plugin 'pem' has unmet soft dependency: CERT_DECODE:PGP
loading feature CERT_DECODE:X509_CRL in plugin 'pem'
  loop detected while loading CERT_DECODE:X509_CRL in plugin 'pem'
  loading feature CERT_DECODE:X509_CRL in plugin 'openssl'
loading feature CERT_DECODE:OCSP_REQUEST in plugin 'pem'
feature CERT_DECODE:OCSP_REQUEST in plugin 'pem' has unmet dependency: CERT_DECODE:OCSP_REQUEST
loading feature CERT_DECODE:OCSP_RESPONSE in plugin 'pem'
loading feature CERT_DECODE:X509_AC in plugin 'pem'
loading feature CERT_DECODE:PKCS10_REQUEST in plugin 'pem'
loading feature CERT_DECODE:PUBKEY in plugin 'pem'
feature CERT_DECODE:PUBKEY in plugin 'pem' has unmet dependency: CERT_DECODE:PUBKEY
loading feature CONTAINER_DECODE:PKCS12 in plugin 'pem'
  loop detected while loading CONTAINER_DECODE:PKCS12 in plugin 'pem'
  loading feature CONTAINER_DECODE:PKCS12 in plugin 'openssl'
loading feature CUSTOM:openssl-threading in plugin 'openssl'
loading feature CRYPTER:AES_CBC-16 in plugin 'openssl'
loading feature CRYPTER:AES_CBC-24 in plugin 'openssl'
loading feature CRYPTER:AES_CBC-32 in plugin 'openssl'
loading feature CRYPTER:CAMELLIA_CBC-16 in plugin 'openssl'
loading feature CRYPTER:CAMELLIA_CBC-24 in plugin 'openssl'
loading feature CRYPTER:CAMELLIA_CBC-32 in plugin 'openssl'
loading feature CRYPTER:CAST_CBC-0 in plugin 'openssl'
loading feature CRYPTER:BLOWFISH_CBC-0 in plugin 'openssl'
loading feature CRYPTER:3DES_CBC-24 in plugin 'openssl'
loading feature CRYPTER:DES_CBC-8 in plugin 'openssl'
loading feature CRYPTER:DES_ECB-8 in plugin 'openssl'
loading feature CRYPTER:NULL-0 in plugin 'openssl'
loading feature HASHER:HASH_MD4 in plugin 'openssl'
loading feature HASHER:HASH_SHA2_224 in plugin 'openssl'
```

```
loading feature HASHER:HASH_SHA2_256 in plugin 'openssl'
loading feature HASHER:HASH_SHA2_384 in plugin 'openssl'
loading feature HASHER:HASH_SHA2_512 in plugin 'openssl'
loading feature PRF:PRF_KEYED_SHA1 in plugin 'openssl'
loading feature PRF:PRF_HMAC_MD5 in plugin 'openssl'
loading feature PRF:PRF_HMAC_SHA1 in plugin 'openssl'
loading feature PRF:PRF_HMAC_SHA2_256 in plugin 'openssl'
loading feature PRF:PRF_HMAC_SHA2_384 in plugin 'openssl'
loading feature PRF:PRF_HMAC_SHA2_512 in plugin 'openssl'
loading feature SIGNER:HMAC_MD5_96 in plugin 'openssl'
loading feature SIGNER:HMAC_MD5_128 in plugin 'openssl'
loading feature SIGNER:HMAC_SHA1_96 in plugin 'openssl'
loading feature SIGNER:HMAC_SHA1_128 in plugin 'openssl'
loading feature SIGNER:HMAC_SHA1_160 in plugin 'openssl'
loading feature SIGNER:HMAC_SHA2_256_128 in plugin 'openssl'
loading feature SIGNER:HMAC_SHA2_256_256 in plugin 'openssl'
loading feature SIGNER:HMAC_SHA2_384_192 in plugin 'openssl'
loading feature SIGNER:HMAC_SHA2_384_384 in plugin 'openssl'
loading feature SIGNER:HMAC_SHA2_512_256 in plugin 'openssl'
loading feature SIGNER:HMAC_SHA2_512_512 in plugin 'openssl'
loading feature AEAD:AES_GCM_16-16 in plugin 'openssl'
loading feature AEAD:AES_GCM_16-24 in plugin 'openssl'
loading feature AEAD:AES_GCM_16-32 in plugin 'openssl'
loading feature AEAD:AES_GCM_12-16 in plugin 'openssl'
loading feature AEAD:AES_GCM_12-24 in plugin 'openssl'
loading feature AEAD:AES_GCM_12-32 in plugin 'openssl'
loading feature AEAD:AES_GCM_8-16 in plugin 'openssl'
loading feature AEAD:AES_GCM_8-24 in plugin 'openssl'
loading feature AEAD:AES_GCM_8-32 in plugin 'openssl'
loading feature DH:ECP_256 in plugin 'openssl'
loading feature DH:ECP_384 in plugin 'openssl'
loading feature DH:ECP_521 in plugin 'openssl'
loading feature DH:ECP_224 in plugin 'openssl'
loading feature DH:ECP_192 in plugin 'openssl'
loading feature DH:ECP_256_BP in plugin 'openssl'
loading feature DH:ECP_384_BP in plugin 'openssl'
loading feature DH:ECP_512_BP in plugin 'openssl'
loading feature DH:ECP_224_BP in plugin 'openssl'
loading feature DH:MODP_3072 in plugin 'openssl'
loading feature DH:MODP_4096 in plugin 'openssl'
loading feature DH:MODP_6144 in plugin 'openssl'
loading feature DH:MODP_8192 in plugin 'openssl'
loading feature DH:MODP_2048 in plugin 'openssl'
loading feature DH:MODP_2048_224 in plugin 'openssl'
loading feature DH:MODP_2048_256 in plugin 'openssl'
loading feature DH:MODP_1536 in plugin 'openssl'
loading feature DH:MODP_1024 in plugin 'openssl'
loading feature DH:MODP_1024_160 in plugin 'openssl'
loading feature DH:MODP_768 in plugin 'openssl'
loading feature DH:MODP_CUSTOM in plugin 'openssl'
loading feature PRIVKEY_GEN:RSA in plugin 'openssl'
loading feature PRIVKEY_SIGN:RSA_EMSA_PKCS1_NULL in plugin 'openssl'
loading feature PUBKEY_VERIFY:RSA_EMSA_PKCS1_NULL in plugin 'openssl'
loading feature PRIVKEY_SIGN:RSA_EMSA_PSS in plugin 'openssl'
loading feature PUBKEY_VERIFY:RSA_EMSA_PSS in plugin 'openssl'
loading feature PRIVKEY_SIGN:RSA_EMSA_PKCS1_SHA1 in plugin 'openssl'
loading feature PUBKEY_VERIFY:RSA_EMSA_PKCS1_SHA1 in plugin 'openssl'
loading feature PRIVKEY_SIGN:RSA_EMSA_PKCS1_SHA2_224 in plugin 'openssl'
loading feature PRIVKEY_SIGN:RSA_EMSA_PKCS1_SHA2_256 in plugin 'openssl'
loading feature PUBKEY_VERIFY:RSA_EMSA_PKCS1_SHA2_224 in plugin 'openssl'
loading feature PUBKEY_VERIFY:RSA_EMSA_PKCS1_SHA2_256 in plugin 'openssl'
loading feature PRIVKEY_SIGN:RSA_EMSA_PKCS1_SHA2_384 in plugin 'openssl'
loading feature PRIVKEY_SIGN:RSA_EMSA_PKCS1_SHA2_512 in plugin 'openssl'
loading feature PUBKEY_VERIFY:RSA_EMSA_PKCS1_SHA2_384 in plugin 'openssl'
loading feature PUBKEY_VERIFY:RSA_EMSA_PKCS1_SHA2_512 in plugin 'openssl'
loading feature PRIVKEY_SIGN:RSA_EMSA_PKCS1_MD5 in plugin 'openssl'
loading feature PUBKEY_VERIFY:RSA_EMSA_PKCS1_MD5 in plugin 'openssl'
loading feature PRIVKEY_DECRYPT:ENCRYPT_RSA_PKCS1 in plugin 'openssl'
loading feature PUBKEY_ENCRYPT:ENCRYPT_RSA_PKCS1 in plugin 'openssl'
loading feature CONTAINER_DECODE:PKCS7 in plugin 'openssl'
loading feature PRIVKEY_GEN:ECDSA in plugin 'openssl'
loading feature PRIVKEY_SIGN:ECDSA_WITH_NULL in plugin 'openssl'
loading feature PUBKEY_VERIFY:ECDSA_WITH_NULL in plugin 'openssl'
loading feature PRIVKEY_SIGN:ECDSA_WITH_SHA1_DER in plugin 'openssl'
loading feature PUBKEY_VERIFY:ECDSA_WITH_SHA1_DER in plugin 'openssl'
```

```
loading feature PRIVKEY_SIGN:ECDSA_WITH_SHA256_DER in plugin 'openssl'
loading feature PUBKEY_VERIFY:ECDSA_WITH_SHA256_DER in plugin 'openssl'
loading feature PRIVKEY_SIGN:ECDSA-256 in plugin 'openssl'
loading feature PUBKEY_VERIFY:ECDSA-256 in plugin 'openssl'
loading feature PRIVKEY_SIGN:ECDSA_WITH_SHA384_DER in plugin 'openssl'
loading feature PRIVKEY_SIGN:ECDSA_WITH_SHA512_DER in plugin 'openssl'
loading feature PUBKEY_VERIFY:ECDSA_WITH_SHA384_DER in plugin 'openssl'
loading feature PUBKEY_VERIFY:ECDSA_WITH_SHA512_DER in plugin 'openssl'
loading feature PRIVKEY_SIGN:ECDSA-384 in plugin 'openssl'
loading feature PRIVKEY_SIGN:ECDSA-521 in plugin 'openssl'
loading feature PUBKEY_VERIFY:ECDSA-384 in plugin 'openssl'
loading feature PUBKEY_VERIFY:ECDSA-521 in plugin 'openssl'
loading feature CUSTOM:revocation in plugin 'revocation'
```

What was your exact plugin list?

> Btw. your *2509-revocation-serials* patch is working fine.

OK, thanks.

#6 - 25.01.2018 22:58 - Luka Logar

I am using version 5.6.1 with some patches here and there.

My plugin list:

```
loaded plugins: charon test-vectors pkcs11 nonce x509 revocation constraints pem openssl curl kernel-netlink s
ocket-default vici updown counters
```

The PUBKEY/ANY_KEY dependency (of *x509* plugin CERT_DECODE:X509 feature) makes all the difference. If I comment it out, then *x509* plugin is used for cert loading. Leave it as it is and *openssl* plugin is used for cert loading?

#7 - 26.01.2018 11:23 - Tobias Brunner

> My plugin list:
> [...]
> The PUBKEY/ANY_KEY dependency (of *x509* plugin CERT_DECODE:X509 feature) makes all the difference. If I comment it out, then *x509* plugin is used for cert loading. Leave it as it is and *openssl* plugin is used for cert loading?

I can't reproduce this. With this plugin list (main difference is the *pkcs11* plugin) I get the load order below and all credentials are parsed by the *x509* plugin.

Plugin features...Plugin features...

```
...
loading feature CUSTOM:pkcs11-certs in plugin 'pkcs11'
  loading feature CERT_DECODE:X509 in plugin 'x509'
    loading feature HASHER:HASH_SHA1 in plugin 'openssl'
    loading feature PUBKEY:ANY in plugin 'pem'
      loop detected while loading PUBKEY:ANY in plugin 'pem'
      loading feature PUBKEY:ANY in plugin 'openssl'
  loading feature CERT_DECODE:X509 in plugin 'pem'
    loop detected while loading CERT_DECODE:X509 in plugin 'pem'
    loading feature CERT_DECODE:X509 in plugin 'openssl'
      loading feature PUBKEY:RSA in plugin 'pem'
        loop detected while loading PUBKEY:RSA in plugin 'pem'
        loading feature PUBKEY:RSA in plugin 'openssl'
      loading feature PUBKEY:ECDSA in plugin 'pem'
        loop detected while loading PUBKEY:ECDSA in plugin 'pem'
        loading feature PUBKEY:ECDSA in plugin 'openssl'
      loading feature PUBKEY:DSA in plugin 'pem'
feature PUBKEY:DSA in plugin 'pem' has unmet dependency: PUBKEY:DSA
      feature CERT_DECODE:X509 in plugin 'openssl' has unmet soft dependency: PUBKEY:DSA
loading feature PRIVKEY:ANY in plugin 'pkcs11'
loading feature NONCE_GEN in plugin 'nonce'
  loading feature RNG:RNG_WEAK in plugin 'openssl'
  loading feature RNG:RNG_STRONG in plugin 'openssl'
...
loading feature CERT_ENCODE:X509_CRL in plugin 'x509'
```

```
loading feature CERT_DECODE:X509_CRL in plugin 'x509'
...
loading feature CUSTOM:revocation in plugin 'revocation'
  loading feature CERT_DECODE:OCSP_RESPONSE in plugin 'pem'
  loading feature CERT_DECODE:X509_CRL in plugin 'pem'
    loop detected while loading CERT_DECODE:X509_CRL in plugin 'pem'
    loading feature CERT_DECODE:X509_CRL in plugin 'openssl'
  loading feature FETCHER:https:// in plugin 'curl'
    loading feature CUSTOM:openssl-threading in plugin 'openssl'
  loading feature FETCHER:http:// in plugin 'curl'
  loading feature FETCHER:ftp:// in plugin 'curl'
  loading feature FETCHER:file:// in plugin 'curl'
...
```

The only difference when commenting out the PUBKEY/KEY_ANY dependency is that these three lines come later (when the features of the *pem* plugin are loaded):

```
    loading feature PUBKEY:ANY in plugin 'pem'
      loop detected while loading PUBKEY:ANY in plugin 'pem'
      loading feature PUBKEY:ANY in plugin 'openssl'
```

I am using version 5.6.1 with some patches here and there.

Now I'm interested in these patches :)

#8 - 26.01.2018 18:31 - Luka Logar

There are no patches to the plugin loading functions, the only patches that may be relevant are to the *openssl* plugin, where most of the unneeded/unwanted algorithms is commented out (more or less only AES128/256-CBC/GCM, SHA1/256/512 and BP ECC are left, no RSA) and RNG_TRUE is added since there is a TRNG (engine loaded via the openssl.cnf).

The plugin loading order is somewhat different than yours:

```
00[DMN] Starting IKE charon daemon (strongSwan 5.6.2dr3, Linux 4.14.14, x86_64)
00[LIB] plugin 'test-vectors': loaded successfully
00[CFG] loaded PKCS#11 v2.20 library 'opensc-pkcs11' (/usr/lib/pkcs11/opensc-pkcs11.so)
00[CFG]   OpenSC Project: OpenSC smartcard framework v0.17
00[CFG]   found token in slot 'opensc-pkcs11':0 (OMNIKEY AG 3121 USB 00 00)
00[CFG]     UserPIN (test) (www.CardContact.de: PKCS#15 emulate)
00[LIB] plugin 'pkcs11': loaded successfully
00[LIB] plugin 'nonce': loaded successfully
00[LIB] plugin 'x509': loaded successfully
00[LIB] plugin 'revocation': loaded successfully
00[LIB] plugin 'constraints': loaded successfully
00[LIB] plugin 'pkcs12': loaded successfully
00[LIB] plugin 'pem': loaded successfully
00[LIB] plugin 'openssl': loaded successfully
00[LIB] plugin 'curl': loaded successfully
00[LIB] plugin 'kernel-netlink': loaded successfully
00[LIB] plugin 'socket-default': loaded successfully
00[LIB] plugin 'vici': loaded successfully
00[LIB] plugin 'updown': loaded successfully
00[LIB] plugin 'counters': loaded successfully
00[LIB] loading feature CUSTOM:libcharon in plugin 'charon'
00[LIB]   loading feature NONCE_GEN in plugin 'nonce'
00[LIB]     loading feature RNG:RNG_WEAK in plugin 'openssl'
00[LIB]   Monobit: 9927/20000 bits set
00[LIB]   Monobit: 9973/20000 bits set
00[LIB]   Poker: 21.056000
00[LIB]   Poker: 3.961600
00[LIB]   Runs: zero: 2529/1289/597/309/172/145, one: 2509/1292/625/313/165/138, longruns: 0
00[LIB]   Runs: zero: 2515/1245/663/310/146/149, one: 2511/1316/588/307/153/154, longruns: 0
00[LIB] enabled  RNG_WEAK[openssl]: passed 3 test vectors
00[LIB]     loading feature RNG:RNG_STRONG in plugin 'openssl'
00[LIB]   Monobit: 9961/20000 bits set
00[LIB]   Monobit: 10077/20000 bits set
00[LIB]   Poker: 13.939200
00[LIB]   Poker: 14.137600
00[LIB]   Runs: zero: 2521/1235/620/315/169/150, one: 2491/1280/627/302/146/163, longruns: 0
00[LIB]   Runs: zero: 2361/1258/654/353/150/166, one: 2541/1180/592/318/143/168, longruns: 0
00[LIB] enabled  RNG_STRONG[openssl]: passed 3 test vectors
00[LIB]     loading feature RNG:RNG_TRUE in plugin 'openssl'
```

```
00[LIB]   Monobit: 9983/20000 bits set
00[LIB]   Monobit: 10147/20000 bits set
00[LIB]   Poker: 7.212800
00[LIB]   Poker: 11.833600
00[LIB]   Runs: zero: 2454/1311/620/315/146/160, one: 2527/1236/630/307/145/161, longruns: 0
00[LIB]   Runs: zero: 2512/1252/599/292/161/166, one: 2507/1228/599/331/146/171, longruns: 0
00[LIB] enabled  RNG_TRUE[openssl]: passed 3 test vectors
00[LIB]   loading feature CUSTOM:libcharon-sa-managers in plugin 'charon'
00[LIB]     loading feature HASHER:HASH_SHA1 in plugin 'openssl'
00[LIB] enabled  HASH_SHA1[openssl]: passed 4 test vectors
00[LIB]   loading feature CUSTOM:libcharon-receiver in plugin 'charon'
00[LIB]     loading feature CUSTOM:socket in plugin 'socket-default'
00[LIB]       loading feature CUSTOM:kernel-ipsec in plugin 'kernel-netlink'
00[LIB]   loading feature CUSTOM:kernel-net in plugin 'kernel-netlink'
00[LIB] loading feature CUSTOM:test-vectors in plugin 'test-vectors'
00[LIB] loading feature CUSTOM:pkcs11-certs in plugin 'pkcs11'
00[LIB]   loading feature CERT_DECODE:X509 in plugin 'x509'
00[LIB]     loading feature PUBKEY:ANY in plugin 'pem'
00[LIB] feature PUBKEY:ANY in plugin 'pem' has unmet dependency: PUBKEY:ANY
00[LIB] feature CERT_DECODE:X509 in plugin 'x509' has unmet dependency: PUBKEY:ANY
00[LIB]   loading feature CERT_DECODE:X509 in plugin 'pem'
00[LIB]     loop detected while loading CERT_DECODE:X509 in plugin 'pem'
00[LIB]     loading feature CERT_DECODE:X509 in plugin 'openssl'
00[LIB]       loading feature PUBKEY:RSA in plugin 'pem'
00[LIB] feature PUBKEY:RSA in plugin 'pem' has unmet dependency: PUBKEY:RSA
00[LIB]       feature CERT_DECODE:X509 in plugin 'openssl' has unmet soft dependency: PUBKEY:RSA
00[LIB]       loading feature PUBKEY:ECDSA in plugin 'pem'
00[LIB]         loop detected while loading PUBKEY:ECDSA in plugin 'pem'
00[LIB]         loading feature PUBKEY:ECDSA in plugin 'openssl'
00[LIB]       loading feature PUBKEY:DSA in plugin 'pem'
00[LIB] feature PUBKEY:DSA in plugin 'pem' has unmet dependency: PUBKEY:DSA
00[LIB]       feature CERT_DECODE:X509 in plugin 'openssl' has unmet soft dependency: PUBKEY:DSA
00[CFG]     loaded untrusted cert 'test'
00[CFG]     loaded trusted cert 'ca'
00[LIB] loading feature PRIVKEY:ANY in plugin 'pkcs11'
00[LIB] loading feature CERT_ENCODE:X509 in plugin 'x509'
00[LIB] loading feature CERT_ENCODE:X509_AC in plugin 'x509'
00[LIB] loading feature CERT_DECODE:X509_AC in plugin 'x509'
00[LIB] loading feature CERT_ENCODE:X509_CRL in plugin 'x509'
00[LIB] loading feature CERT_DECODE:X509_CRL in plugin 'x509'
00[LIB] loading feature CERT_ENCODE:OCSP_REQUEST in plugin 'x509'
00[LIB] loading feature CERT_DECODE:OCSP_RESPONSE in plugin 'x509'
00[LIB] loading feature CERT_ENCODE:PKCS10_REQUEST in plugin 'x509'
00[LIB] loading feature CERT_DECODE:PKCS10_REQUEST in plugin 'x509'
00[LIB] loading feature CUSTOM:revocation in plugin 'revocation'
00[LIB]   loading feature CERT_DECODE:OCSP_RESPONSE in plugin 'pem'
00[LIB]   loading feature CERT_DECODE:X509_CRL in plugin 'pem'
00[LIB]     loop detected while loading CERT_DECODE:X509_CRL in plugin 'pem'
00[LIB]     loading feature CERT_DECODE:X509_CRL in plugin 'openssl'
00[LIB]   loading feature FETCHER:http:// in plugin 'curl'
00[LIB] loading feature CUSTOM:constraints in plugin 'constraints'
00[LIB] loading feature CONTAINER_DECODE:PKCS12 in plugin 'pkcs12'
00[LIB] feature CONTAINER_DECODE:PKCS12 in plugin 'pkcs12' has unmet dependency: CONTAINER_DECODE:PKCS7
00[LIB] loading feature PRIVKEY:ANY in plugin 'pem'
00[LIB]   loop detected while loading PRIVKEY:ANY in plugin 'pem'
00[LIB]   loading feature PRIVKEY:ANY in plugin 'openssl'
00[LIB]   loading feature PRIVKEY:ANY in plugin 'openssl'
00[LIB]   feature PRIVKEY:ANY in plugin 'pem' has unmet soft dependency: HASHER:HASH_MD5
00[LIB] loading feature PRIVKEY:RSA in plugin 'pem'
00[LIB] feature PRIVKEY:RSA in plugin 'pem' has unmet dependency: PRIVKEY:RSA
00[LIB] loading feature PRIVKEY:ECDSA in plugin 'pem'
00[LIB]   loop detected while loading PRIVKEY:ECDSA in plugin 'pem'
00[LIB]   loading feature PRIVKEY:ECDSA in plugin 'openssl'
00[LIB]   feature PRIVKEY:ECDSA in plugin 'pem' has unmet soft dependency: HASHER:HASH_MD5
00[LIB] loading feature PRIVKEY:DSA in plugin 'pem'
00[LIB] feature PRIVKEY:DSA in plugin 'pem' has unmet dependency: PRIVKEY:DSA
00[LIB] loading feature PRIVKEY:BLISS in plugin 'pem'
00[LIB] feature PRIVKEY:BLISS in plugin 'pem' has unmet dependency: PRIVKEY:BLISS
00[LIB] loading feature PRIVKEY:ED25519 in plugin 'pem'
00[LIB] feature PRIVKEY:ED25519 in plugin 'pem' has unmet dependency: PRIVKEY:ED25519
00[LIB] loading feature PUBKEY:BLISS in plugin 'pem'
00[LIB] feature PUBKEY:BLISS in plugin 'pem' has unmet dependency: PUBKEY:BLISS
00[LIB] loading feature PUBKEY:ED25519 in plugin 'pem'
00[LIB] feature PUBKEY:ED25519 in plugin 'pem' has unmet dependency: PUBKEY:ED25519
00[LIB] loading feature CERT_DECODE:ANY in plugin 'pem'
```

```
00[LIB]   loading feature CERT_DECODE:PGP in plugin 'pem'
00[LIB] feature CERT_DECODE:PGP in plugin 'pem' has unmet dependency: CERT_DECODE:PGP
00[LIB]   feature CERT_DECODE:ANY in plugin 'pem' has unmet soft dependency: CERT_DECODE:PGP
00[LIB] loading feature CERT_DECODE:OCSP_REQUEST in plugin 'pem'
00[LIB] feature CERT_DECODE:OCSP_REQUEST in plugin 'pem' has unmet dependency: CERT_DECODE:OCSP_REQUEST
00[LIB] loading feature CERT_DECODE:X509_AC in plugin 'pem'
00[LIB] loading feature CERT_DECODE:PKCS10_REQUEST in plugin 'pem'
00[LIB] loading feature CERT_DECODE:PUBKEY in plugin 'pem'
00[LIB] feature CERT_DECODE:PUBKEY in plugin 'pem' has unmet dependency: CERT_DECODE:PUBKEY
00[LIB] loading feature CONTAINER_DECODE:PKCS12 in plugin 'pem'
00[LIB]   loop detected while loading CONTAINER_DECODE:PKCS12 in plugin 'pem'
00[LIB]   loading feature CONTAINER_DECODE:PKCS12 in plugin 'openssl'
00[LIB] loading feature CUSTOM:openssl-threading in plugin 'openssl'
00[LIB] loading feature CRYPTER:AES_CBC-16 in plugin 'openssl'
00[LIB] enabled  AES_CBC[openssl]: passed 4 test vectors
00[LIB] loading feature CRYPTER:AES_CBC-24 in plugin 'openssl'
00[LIB] enabled  AES_CBC[openssl]: passed 1 test vectors
00[LIB] loading feature CRYPTER:AES_CBC-32 in plugin 'openssl'
00[LIB] enabled  AES_CBC[openssl]: passed 1 test vectors
00[LIB] loading feature HASHER:HASH_SHA2_256 in plugin 'openssl'
00[LIB] enabled  HASH_SHA2_256[openssl]: passed 3 test vectors
00[LIB] loading feature HASHER:HASH_SHA2_512 in plugin 'openssl'
00[LIB] enabled  HASH_SHA2_512[openssl]: passed 3 test vectors
00[LIB] loading feature PRF:PRF_HMAC_SHA2_256 in plugin 'openssl'
00[LIB] enabled  PRF_HMAC_SHA2_256[openssl]: passed 6 test vectors
00[LIB] loading feature PRF:PRF_HMAC_SHA2_512 in plugin 'openssl'
00[LIB] enabled  PRF_HMAC_SHA2_512[openssl]: passed 6 test vectors
00[LIB] loading feature SIGNER:HMAC_SHA2_256_128 in plugin 'openssl'
00[LIB] enabled  HMAC_SHA2_256_128[openssl]: passed 3 test vectors
00[LIB] loading feature SIGNER:HMAC_SHA2_256_256 in plugin 'openssl'
00[LIB] disabled HMAC_SHA2_256_256[openssl]: no test vectors found
00[LIB] loading feature SIGNER:HMAC_SHA2_512_256 in plugin 'openssl'
00[LIB] enabled  HMAC_SHA2_512_256[openssl]: passed 3 test vectors
00[LIB] loading feature SIGNER:HMAC_SHA2_512_512 in plugin 'openssl'
00[LIB] disabled HMAC_SHA2_512_512[openssl]: no test vectors found
00[LIB] loading feature AEAD:AES_GCM_16-16 in plugin 'openssl'
00[LIB] enabled  AES_GCM_16[openssl]: passed 5 test vectors
00[LIB] loading feature AEAD:AES_GCM_16-24 in plugin 'openssl'
00[LIB] enabled  AES_GCM_16[openssl]: passed 5 test vectors
00[LIB] loading feature AEAD:AES_GCM_16-32 in plugin 'openssl'
00[LIB] enabled  AES_GCM_16[openssl]: passed 5 test vectors
00[LIB] loading feature DH:ECP_256_BP in plugin 'openssl'
00[LIB] enabled  ECP_256_BP[openssl]: passed 1 test vectors
00[LIB] loading feature DH:ECP_384_BP in plugin 'openssl'
00[LIB] enabled  ECP_384_BP[openssl]: passed 1 test vectors
00[LIB] loading feature DH:ECP_512_BP in plugin 'openssl'
00[LIB] enabled  ECP_512_BP[openssl]: passed 1 test vectors
00[LIB] loading feature PRIVKEY_GEN:ECDSA in plugin 'openssl'
00[LIB] loading feature PRIVKEY_SIGN:ECDSA_WITH_NULL in plugin 'openssl'
00[LIB] loading feature PUBKEY_VERIFY:ECDSA_WITH_NULL in plugin 'openssl'
00[LIB] loading feature PRIVKEY_SIGN:ECDSA_WITH_SHA1_DER in plugin 'openssl'
00[LIB] loading feature PUBKEY_VERIFY:ECDSA_WITH_SHA1_DER in plugin 'openssl'
00[LIB] loading feature PRIVKEY_SIGN:ECDSA_WITH_SHA256_DER in plugin 'openssl'
00[LIB] loading feature PUBKEY_VERIFY:ECDSA_WITH_SHA256_DER in plugin 'openssl'
00[LIB] loading feature PRIVKEY_SIGN:ECDSA-256 in plugin 'openssl'
00[LIB] loading feature PUBKEY_VERIFY:ECDSA-256 in plugin 'openssl'
00[LIB] loading feature PRIVKEY_SIGN:ECDSA_WITH_SHA512_DER in plugin 'openssl'
00[LIB] loading feature PUBKEY_VERIFY:ECDSA_WITH_SHA512_DER in plugin 'openssl'
00[LIB] loading feature CUSTOM:vici in plugin 'vici'
00[LIB]   loading feature CUSTOM:counters in plugin 'counters'
00[CFG] crl caching to /etc/swanctl/x509crl enabled
00[LIB] loading feature CUSTOM:updown in plugin 'updown'
00[LIB] unloading plugin 'pkcs12' without loaded features
00[LIB] loaded plugins: charon test-vectors pkcs11 nonce x509 revocation constraints pem openssl curl kernel-n
etlink socket-default vici updown counters
```

#9 - 29.01.2018 09:59 - Tobias Brunner

There are no patches to the plugin loading functions, the only patches that may be relevant are to the *openssl* plugin, where most of the unneeded/unwanted algorithms is commented out (more or less only AES128/256-CBC/GCM, SHA1/256/512 and BP ECC are left, no RSA) and RNG_TRUE is added since there is a TRNG (engine loaded via the openssl.cnf).

Well, that included the PUBKEY:ANY feature provided by the *openssl* plugin (source:src/libstrongswan/plugins/openssl/openssl_plugin.c#L622) and since you don't load the *pkcs1* plugin this means the cert decoding of the *x509* plugin won't be available (no matter the plugin order, the only thing you can control in this case is which plugin parses the CRLs first). So that explains what you are seeing.

#10 - 31.01.2018 10:53 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to Fixed

Files

strongswan-openssl-serialnum.patch	1.58 KB	07.01.2018	Luka Logar