

New issue

Jump to bottom

It may not be necessary to check the "revocation date" #3340

Closed yuemonangong opened this issue on May 21, 2020 · 1 comment · Fixed by #3433

Labels bug component-x509

yuemonangong commented on May 21, 2020

Description

- Type: Bug

Bug

OS
ubuntu 16.04.1 [linux]

mbed TLS build:
Version: 2.16.5

I created a CRL whose revocation date is later than current time. MbedTLS does not use this CRL because it thought that the CRL is illegal (see the code in /library/x509_crt.c, line 1788). Comparatively, openssl does not check the "revocation date" field and revokes certificate(s).

The openssl guys explained that "revocation date" is useless in certificate validation and may only be used as meta data (see [openssl/openssl#11859](#)). I indeed checked RFC 5280 and did not find any words saying that "revocation date" is important (for certificate parsing and validation). Then do we still need to check the revocation date?

```
#if defined(MBEDTLS_X509_CRL_PARSE_C)
/*
 * Return 1 if the certificate is revoked, or 0 otherwise.
 */
int mbedtls_x509_crt_is_revoked( const mbedtls_x509_crt *crt, const mbedtls_x509_crl *crl )
{
    const mbedtls_x509_crl_entry *cur = &crl->entry;

    while( cur != NULL && cur->serial.len != 0 )
    {
        if( crt->serial.len == cur->serial.len &&
            memcmp( crt->serial.p, cur->serial.p, crt->serial.len ) == 0 )
        {
            if( mbedtls_x509_time_is_past( &cur->revocation_date ) )
                return( 1 );
        }

        cur = cur->next;
    }

    return( 0 );
}
```

The command I used is:

```
cert_app mode='file' filename=leaf.pem ca_file=root.pem crl_file=test.crl
```

The verification returns

```
Result of MbedTLS:
. Loading the CA root certificate ... ok (0 skipped)

. Loading the certificate(s) ... ok
. Peer certificate information ...
  cert. version      : 3
  serial number      : 01
  issuer name         : C=CN, ST=SH, O=SJTU, OU=DDST, CN=NCRL
  subject name        : C=GB, ST=Berkshire, L=Newbury, O=My Company Ltd
  issued on           : 1996-08-01 00:00:00
  expires on           : 2020-12-31 23:59:59
  signed using         : RSA with SHA-256
  RSA key size         : 2048 bits
  basic constraints    : CA=true

. Verifying X.509 certificate...
Verify requested for (Depth 1):
cert. version      : 3
serial number      : F5:34:01:4D:DA:77:4E:2F
issuer name         : C=CN, ST=SH, O=SJTU, OU=DDST, CN=NCRL
subject name        : C=CN, ST=SH, O=SJTU, OU=DDST, CN=NCRL
issued on           : 2020-03-26 08:27:49
expires on           : 2023-01-14 08:27:49
signed using         : RSA with SHA-256
RSA key size         : 2048 bits
basic constraints    : CA=true, max_pathlen=3
key usage            : Digital Signature, Non Repudiation, Key Encipherment, Key Cert Sign, CRL Sign
This certificate has no flags

Verify requested for (Depth 0):
cert. version      : 3
serial number      : 01
issuer name         : C=CN, ST=SH, O=SJTU, OU=DDST, CN=NCRL
subject name        : C=GB, ST=Berkshire, L=Newbury, O=My Company Ltd
```

```
issued on      : 1996-08-01 00:00:00
expires on     : 2020-12-31 23:59:59
signed using   : RSA with SHA-256
RSA key size   : 2048 bits
basic constraints : CA=true
               This certificate has no flags
ok
```

Result of OpenSSL:

```
C = GB, ST = Berkshire, L = Newbury, O = My Company Ltd
error 23 at 0 depth lookup: certificate revoked
error leaf.pem: verification failed
```

root.pem

```
-----BEGIN CERTIFICATE-----
MIIDNDCCAhYgAwIBAgIJApu8AU3ad04vMA0GC5qGSIb3DQECCwJAMecxZAJBgNV
BAYTANOMQSwCQYDVQQIDAJTSDENMAsGA1UECgwEU0pUTENMAsGA1UECwwERERT
VDENMAsGA1UEAwETkNSTDAeFw0yMDA2MjYwODI3NDI1aFw0yMDA2MjYwODI3NDI1a
MEcxZAJBgNVBAYTANOMQSwCQYDVQQIDAJTSDENMAsGA1UECgwEU0pUTENMAsGA1
UECwwERERTVDENMAsGA1UEAwETkNSTDCCAS1w0QYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAPNLlu+KPCcj1KiZ1/sUFvFRDt3Z7WZTWj0Ye3UfvyCHNcYN9cE
1aGJ32hfjgaPh9u3c0gs0JJHwIh1QKnhSexUvgGatw336H/3FjPQCJKs48IDJG13
sDF7TK1MvG5wcF1pgRkFv0rSW0yr30aqoeQhArngMt8lWByZ6mmV6mgM7LPeNq8
E6jh6aLy7uep3+r0/Ef7LvFi/QWqy+vVmr5M1jXtFyWl+aLs4uFtZZGrFw5Va4U
Y60ffwchjkVex1eML4D593fobknubxZEm2o2Up1/Eiech7CM8HuwgqrAwoIVx16
F10braD90sUSUKUwhv103tkjCTXakXF2TUCAwEAAAMjMCEwEgYDVR0IQAQ/BAgw
BgEB/wI8AzaALBgnVHQ8EBAMCAeYwDQYJKoZIhvcNAQELBQADggEBACb6hOtUcqD5
sH4VucCO4FYFHm6nFbV9vxx+c2RPPC/psam9c10vL511rUhy070pXbZnd2hwxfnzj
cdr448svYjKhosukzZj/MyEBV9BERTUM0ay4etQxM2L33uyzn5++/NeRC2Yd53AL
vY/s4znat7txqBK/izvLemLerp1ZSE58VFzLOvNz+7vEoxMmNaUSGh88VJ1Ivo
THaZ3LF1Tc7hV9eLMin0LTV0mg7cvM+/qlmM2N2hyQukztF5GcMEgoVkpEgUCIP
WsrvoUmtDNuXnPr80r4NS4n5TaQCTBG22Tj89k1c6juji63+UR9KKACCV44KT8hc
+0ecJPMxqEU=
-----END CERTIFICATE-----
```

leaf.pem

```
-----BEGIN CERTIFICATE-----
MIIDITCCAgmgAwIBAgIBATANBgkqhkiG9w0BAQsFADBBMQSwCQYDVQQGEwJDTjEL
MAkGA1UECAwCU0gxDALBgnVBAAoMBFNKVfUxDALBgnVBAsMBEREU1QxDALBgnV
BAMMBESDUkwthhcN0TYwODAXMDAwMDAwthcNMjYwODI3NDI1OTU5wJBMQSwCQYD
VQQGEwJHQjESMBAGAA1UECBMjQmVya3NoaXJlMRAwDgYDVQQHEwD0ZXd1dXJ3MRCw
FOYDVQQKEw5MeSB0b21wYw55IE80ZDCCAS1w0QYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAL+N8yeP181T/+MxN/311Behb2r05s8MzykUz3aGp3BG/SuEFueqoYZN
CNLA38wIUT/ry8wIw+j1TNj29L7Q9uOX8+10XgF4VTvtN14KT0s7tZ5dLJGRD7ft
fZF03ifbGYp39f9W2WjutJo4Jyop+Bm7g65r5J3B3uaIoITpZ8Xf7MH0+kNJJKPsu
Z1VvNQ3TSWQz0skcpRRiUjv7U/NATuRzXODUzqnm+HGavu2qTX3Falo510dzzrT
9yCtLkQtC+00x+kZP1i3ib/o20FY3hEXwStq5sKpvV25xgKTbtwRN1K1MIhF5QN
uFXIg/Rd6rbdb9P60zPYxzOTwMsaEysECAwEAAAMTMBEwDwYDVROTAQH/BAUwAwEB
/zaNBgkqhkiG9w0BAQsFAA0CAQEAKhf5CQGsJczKfJv26ggzi2HxN/X/eXcwJyy
3gfPP0JZNLzRb6bmraCLu158LYCX+0tmY5TA1G3V94Vdu2LIUMRoANwKszTxHw/n
80NvXDji+E6ZesivCtPogYRAwFE04f1vcWzDwG1qCFdaG1uqGL1LxW8gmHdFs
pkJf4yCzQ0n84RmReXohaAtyUT+xp9AUzawzr2PPGA75x7B07HT4ezLPWY+11X8o
gMB0Mm3AwrwTD8k1B488N1KivCYjBn6UPG0r9/gKXsVdE3EJ6SYM8+Jw+f71jJ8i
55LYq8BoypPKnQ0AwZB+KZkCbqkcBGJLEPR35agBN/S0S5dioXA==
-----END CERTIFICATE-----
```

test.crl

```
-----BEGIN X509 CRL-----
MIIBTjCBnwIBATANBgkqhkiG9w0BAQ4FADBBMQSwCQYDVQQGEwJDTjELMAkGA1UE
CAwCU0gxDALBgnVBAAoMBFNKVfUxDALBgnVBAsMBEREU1QxDALBgnVBAMMBE5D
UkwXDTIwMDMwODIwIwMjYwN1oXDTIxMDIyMTIwMjYwN1owFASAgEBFw0yMTAyMjE
yMDI2MDda0A4wDAKBgNVHRQEAwIBADANBgkqhkiG9w0BAQ4FAA0CAQEAKqQPjXyG
FTYpH147KoMaeg0W7uJ5K08SXOHxUEU65+QuXOK5p0SpjAH+JhLkSH19dY+22gW
+8ec3N3P02Iw7IK58t5j1+Uywr13VnF6g2Pf+7zr2je3XoTHATLp+LHFVkuJL1f1Z
/FiEtJ56NVsNemrAY+BNCCIOcHqBVjMAX1zSmlUw91SUFiH6+9H0tVQ0FI0MSRBA5
60oCmA03t/5FZF3LqxGj5z3weBvS4301ebf20remV2pEFwMh9KKDBKx+Rd9njgW
dmrKKY4pLFAUZ+D2eCevHBU7vL55jmg80Ku+74/128wGF+70Ftj5tcbk4hdcj11
/gX0RqNhgLarQw==
-----END X509 CRL-----
```

  gilles-peskin-arm mentioned this issue on Aug 11, 2020

Always revoke certificate on CRL #3433


 Merged


 4 tasks

gilles-peskin-arm commented on Aug 11, 2020

Contributor

Thanks for reporting this! As it happens there's a fix pending, which we hope to merge soon: #3433 .

  gilles-peskin-arm added `bug` `component-x509` `fix available` labels on Aug 11, 2020

 gilles-peskin-arm closed this as completed in #3433 on Aug 26, 2020

Assignees

No one assigned

Labels

bug **component-x509**

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 **Always revoke certificate on CRL**
raulstrackx/mbedtls

2 participants

