strongSwan - Issue #2628

"crl fetched successfully but parsing failed" when use CRL

12.04.2018 05:18 - Bin Liu

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	libstrongswan		
Affected version:	5.3.3	**Resolution:**	Duplicate

Description

Hi,
I have a trouble when use CRL to check cert status,the log is as follow:

```
Apr 12 10:21:32 LTE-GW charon: 13[CFG] checking certificate status of "CN=Henb"
Apr 12 10:21:32 LTE-GW charon: 13[CFG]   fetching crl from 'http://10.252.1.77:8080/ejbca/publicwe
b/webdist/certdist?cmd=crl&format=PEM&issuer=CN%3DTest-RootCA' ...
Apr 12 10:21:32 LTE-GW charon: 13[LIB] building CRED_CERTIFICATE - X509_CRL failed, tried 4 builde
rs
Apr 12 10:21:32 LTE-GW charon: 13[CFG] crl fetched successfully but parsing failed
Apr 12 10:21:32 LTE-GW charon: 13[CFG] certificate status is not available
```

The http url for CRLs is available, i can download the CRL file, and also i can use openssl or ipsec command to parse it.

Please help me,thanks.

Here are more informations:
---
ipsec plugins loaded:

```
ipsec statusall
Status of IKE charon daemon (strongSwan 5.3.3, Linux 3.12.20, x86_64):
  uptime: 59 minutes, since Apr 12 09:55:24 2018
  malloc: sbrk 405504, mmap 0, used 330032, free 75472
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 0
  loaded plugins: charon aes des gmp hmac md5 nonce random sha1 sha2 xcbc constraints pem pgp pkcs
1 pkcs7 pkcs8 pkcs12 pubkey x509 curl openssl revocation fips-prf attr kernel-netlink resolve sock
et-default stroke updown eap-aka eap-identity eap-radius
```

---
use openssl to parse crl file:

```
openssl crl -noout -text -in Test-RootCA.crl
Certificate Revocation List (CRL):
        Version 2 (0x1)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: /CN=Test-RootCA
        Last Update: Apr 11 07:54:36 2018 GMT
        Next Update: Apr 12 07:54:36 2018 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
                keyid:F3:C3:85:68:94:D1:AD:2D:BB:93:28:2F:A0:08:F7:E3:9A:63:0C:D9

            X509v3 CRL Number:
                5
Revoked Certificates:
    Serial Number: 6DEB7153D31F5250
        Revocation Date: Apr  8 07:41:45 2018 GMT
    Serial Number: 20A733BC952693D8
        Revocation Date: Apr  9 10:00:14 2018 GMT
    Serial Number: 5F0FFCB8945B20D5
        Revocation Date: Apr  9 10:00:13 2018 GMT
```

```
    Serial Number: 0CB54A512387D118
        Revocation Date: Apr  9 10:00:14 2018 GMT
    Serial Number: 2DF5AE351D498A45
        Revocation Date: Apr  9 11:04:58 2018 GMT
    Serial Number: 51858293F3373911
        Revocation Date: Apr  8 06:59:47 2018 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                AA Compromise
    Serial Number: 2753963259D00AA9
        Revocation Date: Apr  9 11:53:45 2018 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 40B670043C7A17F3
        Revocation Date: Apr  9 10:00:13 2018 GMT
    Serial Number: 261567C83EDC5ECD
        Revocation Date: Apr  8 07:41:45 2018 GMT
    Serial Number: 4BA3A0A0552BB1DC
        Revocation Date: Apr  9 10:00:14 2018 GMT
    Serial Number: 2105E187854CA9A0
        Revocation Date: Apr  9 11:12:46 2018 GMT
    Serial Number: 402618DBDA686B85
        Revocation Date: Apr  8 06:59:47 2018 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                AA Compromise
    Serial Number: 04E633474786A4F9
        Revocation Date: Apr  9 11:12:46 2018 GMT
    Serial Number: 7716F7C7F160DE80
        Revocation Date: Apr  9 11:04:58 2018 GMT
    Serial Number: 328EFACD02486234
        Revocation Date: Apr  9 11:12:46 2018 GMT
    Serial Number: 5170AF43614B9FF8
        Revocation Date: Apr  9 10:00:14 2018 GMT
    Serial Number: 5CABBA6616B128FE
        Revocation Date: Apr  9 11:12:46 2018 GMT
    Serial Number: 46D9E04D074E2570
        Revocation Date: Apr  9 11:04:58 2018 GMT
    Serial Number: 3E80AFC300E80962
        Revocation Date: Apr  9 11:04:58 2018 GMT
    Signature Algorithm: sha1WithRSAEncryption
         09:78:24:ec:e6:3e:86:75:c7:44:86:7f:15:47:40:23:ed:ff:
         58:f8:f3:60:a7:e3:1e:9e:4f:99:c7:62:29:8e:7f:2c:5c:3a:
         14:af:f3:c2:a0:f8:23:13:9d:e3:22:5a:1e:52:5f:8f:b6:70:
         7a:55:c9:8f:c1:2c:f7:88:59:d4:3b:08:70:95:09:8a:32:47:
         91:f0:a9:8f:30:87:46:d0:48:b8:91:19:9a:54:95:53:dd:6f:
         f9:14:b5:dd:4c:ae:08:de:1f:43:aa:db:92:78:1a:b8:6e:29:
         07:a6:31:b4:0a:6c:c8:8d:e8:d0:7b:9f:2c:ad:ef:4d:59:7d:
         52:5a:61:3e:fd:97:c6:d6:77:94:21:e1:13:4e:91:66:ea:ac:
         96:b6:8e:ec:41:9b:e6:48:4c:fd:ac:ee:b8:cd:46:b5:e0:a9:
         46:34:09:81:a0:69:75:2d:f0:56:1a:6b:4f:d8:1f:0f:1b:ca:
         fb:9a:b4:61:13:2d:19:b6:99:12:ed:3b:a7:b6:00:e3:29:ec:
         7d:ae:68:23:f5:22:16:20:b0:d4:59:2d:14:78:78:88:dc:f1:
         59:6d:fd:78:d0:58:f7:66:d8:df:c2:da:30:34:13:97:84:1b:
         9f:10:40:21:b2:ab:27:9d:04:9e:2b:48:bc:73:99:33:a9:29:
         9e:f0:76:86
```

---

use ipsec to parse crl file:

```
ipsec pki --print -t crl -i Test-RootCA.crl
cert:      X509_CRL
issuer:   "CN=Test-RootCA"
validity:  not before Apr 11 15:54:36 2018, ok
           not after  Apr 12 15:54:36 2018, ok (expires in 5 hours)
```

```
serial:    05
authKeyId: f3:c3:85:68:94:d1:ad:2d:bb:93:28:2f:a0:08:f7:e3:9a:63:0c:d9
19 revoked certificates:
    6d:eb:71:53:d3:1f:52:50 unspecified 2018-04-08 15:41:45
    20:a7:33:bc:95:26:93:d8 unspecified 2018-04-09 18:00:14
    5f:0f:fc:b8:94:5b:20:d5 unspecified 2018-04-09 18:00:13
    0c:b5:4a:51:23:87:d1:18 unspecified 2018-04-09 18:00:14
    2d:f5:ae:35:1d:49:8a:45 unspecified 2018-04-09 19:04:58
    51:85:82:93:f3:37:39:11 (10) 2018-04-08 14:59:47
    27:53:96:32:59:d0:0a:a9 cessation of operation 2018-04-09 19:53:45
    40:b6:70:04:3c:7a:17:f3 unspecified 2018-04-09 18:00:13
    26:15:67:c8:3e:dc:5e:cd unspecified 2018-04-08 15:41:45
    4b:a3:a0:a0:55:2b:b1:dc unspecified 2018-04-09 18:00:14
    21:05:e1:87:85:4c:a9:a0 unspecified 2018-04-09 19:12:46
    40:26:18:db:da:68:6b:85 (10) 2018-04-08 14:59:47
    04:e6:33:47:47:86:a4:f9 unspecified 2018-04-09 19:12:46
    77:16:f7:c7:f1:60:de:80 unspecified 2018-04-09 19:04:58
    32:8e:fa:cd:02:48:62:34 unspecified 2018-04-09 19:12:46
    51:70:af:43:61:4b:9f:f8 unspecified 2018-04-09 18:00:14
    5c:ab:ba:66:16:b1:28:fe unspecified 2018-04-09 19:12:46
    46:d9:e0:4d:07:4e:25:70 unspecified 2018-04-09 19:04:58
    3e:80:af:c3:00:e8:09:62 unspecified 2018-04-09 19:04:58
```

---

ipsec listplugins,see attachments

---

crl file,see attachments

Related issues:

Related to Bug #1203: Unable to fetch CRL from files with the curl plugin (or...	**Closed**	**10.11.2015**

History

#1 - 12.04.2018 10:38 - Tobias Brunner

- Status changed from New to Feedback

The most likely reason for the parsing to fail is that whatever is fetched from that URL is not the CRL you were able to successfully parse. Did you actually try to e.g. use

```
wget http://10.252.1.77:8080/ejbca/publicweb/webdist/certdist?cmd=crl&format=PEM&issuer=CN%3DTest-RootCA
```

or

```
curl http://10.252.1.77:8080/ejbca/publicweb/webdist/certdist?cmd=crl&format=PEM&issuer=CN%3DTest-RootCA
```

to see what you get back?

#2 - 12.04.2018 10:59 - Bin Liu

- File crl.pcap added

Yes, we have tried,because there are '&' character in the uri,the result looks a little strange.
use curl:

```
[root@LTE-GW crls]# curl 'http://10.252.1.77:8080/ejbca/publicweb/webdist/certdist?cmd=crl&format=PEM&issuer=C
N%3DTest-RootCA'
-----BEGIN X509 CRL-----
MIIDwDCCAqgCAQEwDQYJKoZIhvcNAQEFBQAwFjEUMBIGA1UEAxMLVGVzdC1Sb290
Q0EXDTE4MDQxMTA3NTQzNloXDTE4MDQxMjA3NTQzNlowggIrMBkCCG3rcVPTH1JQ
Fw0xODA0MDgwNzQxNDVaMBkCCCCnM7yVJpPYFw0xODA0MDkxMDAwMTRaMBkCCF8P
/LiUWyDVFw0xODA0MDkxMDAwMTNaMBkCCAy1SlEjh9EYFw0xODA0MDkxMDAwMTRa
MBkCCC31rjUdSYpFFw0xODA0MDkxMTA0NThaMCcCCFGFgpPzNzkRFw0xODA0MDgw
NjU5NDdaMAwwCgYDVR0VBAMKAQowJwIIJ1OWMlnQCqkXDTE4MDQwOTExNTM0NVow
DDAKBgNVHRUEAwoBBTAZAghAtnAEPHoX8xcNMTgwNDA5MTAwMDEzWjAZAggmFWfI
PtxezRcNMTgwNDA4MDc0MTQ1WjAZAghLo6CgVSux3BcNMTgwNDA5MTAwMDE0WjAZ
AgghBeGHhUypoBcNMTgwNDA5MTExMjQ2WjAnAghAJhjb2mhrhRcNMTgwNDA4MDY1
OTQ3WjAMMAoGA1UdFQQDCgEKMBkCCATmM0dHhqT5Fw0xODA0MDkxMTEyNDZaMBkC
CHcW98fxYN6AFw0xODA0MDkxMTA0NThaMBkCCDKO+s0CSGI0Fw0xODA0MDkxMTEy
```

```
NDZaMBkCCFFwr0NhS5/4Fw0xODA0MDkxMDAwMTRaMBkCCFyrumYWsSj+Fw0xODA0
MDkxMTEyNDZaMBkCCEbZ4E0HTiVwFw0xODA0MDkxMTA0NThaMBkCCD6Ar8MA6Ali
Fw0xODA0MDkxMTA0NThaoC8wLTAfBgNVHSMEGDAWgBTzw4VolNGtLbuTKC+gCPfj
mmMM2TAKBgNVHRQEAwIBBTANBgkqhkiG9w0BAQUFAAOCAQEACXgk7OY+hnXHRIZ/
FUdAI+3/WPjzYKfjHp5PmcdiKY5/LFw6FK/zwqD4IxOd4yJaHlJfj7ZwelXJj8Es
94hZ1DsIcJUJijJHkfCpjzCHRtBIuJEZmlSVU91v+RS13UyuCN4fQ6rbkngauG4p
B6YxtApsyI3o0HufLK3vTVl9UlphPv2XxtZ3lCHhE06RZuqslraO7EGb5khM/azu
uM1GteCpRjQJgaBpdS3wVhprT9gfDxvK+5q0YRMtGbaZEu07p7YA4ynsfa5oI/Ui
FiCw1FktFHh4iNzxWW39eNBY92bY38LaMDQTl4QbnxBAIbKrJ50EnitIvHOZM6kp
nvB2hg==
-----END X509 CRL-----

[3]+  Stopped                 more certdist?cmd=crl
[4]   Done                    format=PEM
[root@LTE-GW crls]#
```

or use wget :

```
[root@LTE-GW crls]# wget 'http://10.252.1.77:8080/ejbca/publicweb/webdist/certdist?cmd=crl&format=PEM&issuer=C
N%3DTest-RootCA'
--2018-04-12 16:44:07--  http://10.252.1.77:8080/ejbca/publicweb/webdist/certdist?cmd=crl&format=PEM&issuer=CN
%3DTest-RootCA
Connecting to 10.252.1.77:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1357 (1.3K) [application/octet-stream]
Saving to: â€œcertdist?cmd=crl&format=PEM&issuer=CN=Test-RootCAâ€

100%[=======================================================================================================
=============================================================================>] 1,357       --.-K/s
  in 0s

2018-04-12 16:44:07 (307 MB/s) - â€œcertdist?cmd=crl&format=PEM&issuer=CN=Test-RootCAâ€ saved [1357/1357]
```

But we have downloaded the CRL actually.
During creating IPSec connection ,we have captured the http packet, the response is ok,see attachment.

#3 - 12.04.2018 11:04 - Tobias Brunner

Ah, I see. Your problem is the PEM encoding, see #1203 for details (PEM-encoded, fetched CRLs are supported since 5.3.4).

#4 - 12.04.2018 11:04 - Tobias Brunner

- Related to Bug #1203: Unable to fetch CRL from files with the curl plugin (or in PEM format) added

#5 - 12.04.2018 11:13 - Bin Liu

OK,thanks a lot.

#6 - 12.04.2018 11:31 - Tobias Brunner

- Category set to libstrongswan

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to Duplicate

Files

Test-RootCA.crl	1.33 KB	12.04.2018	Bin Liu
ipsec listplugins.txt	10.3 KB	12.04.2018	Bin Liu
crl.pcap	459 KB	12.04.2018	Bin Liu