strongSwan - Feature #2366

let crl-fetcher follow redirects

24.06.2017 22:27 - Andreas Marx

Status:	Closed	**Start date:**	24.06.2017
Priority:	Low	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libstrongswan		
Target version:	5.6.0		
Resolution:	Fixed		

Description

curl_fetcher does not set Option CURLOPT_FOLLOWLOCATION, so if the CRL-distribution-point is redirected, ipsec pki fails to download the certificate revocation list.

Please set this option. There is no security impact IMHO, since the CRL is signed anyway. Not doing so inhibits the use of some cloud services (dropbox et al.) to distribute the CRL.

Associated revisions

Revision 67402ec7 - 27.07.2017 13:15 - Tobias Brunner

curl: Enable following redirects

The maximum number of redirects can be limited. The functionality can also
be disabled.

Fixes #2366.

History

#1 - 26.06.2017 10:33 - Tobias Brunner

- Category changed from pki to libstrongswan

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

- Target version set to 5.6.0

> ipsec pki fails to download the certificate revocation list.

Are you using pki --verify?

> There is no security impact IMHO, since the CRL is signed anyway.

I guess not, unless it gets easier for an attacker to prevent a host from getting the CRL in the first place (if strict CRL checking is not used the unavailability of a CRL is not an error). I suppose we could make it configurable, in case it causes problems, see *2366-curl-redirects* branch.

#2 - 26.06.2017 17:42 - Andreas Marx

I am using **ipsec scepclient** to enroll to a sub-CA. Both, the intermediate and the root, are issuing certs with crl distribution points set. This command fetched one CRL to /etc/ipsec.d/crls/ (hosted without redirect), but failed for the other one. Fetching the CRL with the curl-commend also failed, unless I fetched with option **-L**.

I do use strict crl checking, I want to be able to revoke the intermediate CA (which has internet connectivity) if it gets breached. My root CA has strict one-way communication to the internet, it just publishes CRLs via dropbox.

I hope I find the time to test your branch this week.

#3 - 27.06.2017 23:41 - Andreas Marx

I have tested 50c129b8072ffd1065aad3964cb8ad7710130687 successfully for my setup. Excerpt from **ipsec up** output (slightly anonymized):

```
checking certificate status of "C=de, O=xxxx, CN=XXXX"
  fetching crl from 'https://dl.dropbox.com/s/YYYYYYoldriv/crl.crl' ...
  using trusted certificate "C=de, O=xxxx, CN=XXXXX"
  crl correctly signed by "C=de, O=xxxx, CN=XXXXX"
  crl is valid: until Jul 22 21:07:45 2017
certificate status is good
  reached self-signed root ca with a path length of 1
```

Exactly this fetch failed previously, the downloaded file contained the redirect headers instead of the CRLs content.

#4 - 29.06.2017 16:58 - Tobias Brunner

> I have tested 50c129b8072ffd1065aad3964cb8ad7710130687 successfully for my setup.

OK, great. Thanks for testing. This will probably be included in the next release.

#5 - 08.08.2017 18:00 - Tobias Brunner

- Status changed from Feedback to Closed

- Resolution set to Fixed