strongSwan - Bug #1203

Unable to fetch CRL from files with the curl plugin (or in PEM format)

10.11.2015 20:04 - Alex Brew

Status:	Closed	**Start date:**	10.11.2015
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libstrongswan		
Target version:	5.3.4		
Affected version:	5.3.3	**Resolution:**	Fixed

Description

I have 5.3.3 built in my own at Ubuntu 14.04 LTS x32.
It is built with also curl and files plugins.
I have OpenSSL generated Root->Intermediate->Server/Clients certificate with Crls by me.
I want to put as Root/Intermediate certificates as its Crls to non-default location, for example to /var/ca/myca and want to fetch Crls from files.
To get such solution working when certificates and Crls are at non-default location with Crls fetching from files is necessary:
- Strongswan must be built with files pluging or this plugin must be installed in case of repo installation;
- files plugin must be specified at load parameter in stronswan.conf;
- files plugin must be specified before curl plugin if there is, at stronswan.conf;
- each CA certificate: for example Root and Intermediate certificate to be specified as cacert parameter at "ca" section in ipsec.conf;
- each Crl have to be specified trhough crluri parameter at "ca" section in ipsec.conf;
- all necessary Crls must be in DER format.

So, I offer to dev team to make Crl fetching from file easier by adding parameter, for example, "crl" to ipsec.conf where path to Crl have to be put and handle Crl fetching from non-default location as if it would be at default location and in Pem format and without curl or files plugins.

As I saw that Crls located at default location is fetched from file without plugings (at least without files plugin) and in Pem format as well.

Related issues:

Related to Issue #2628: "crl fetched successfully but parsing failed" when us...	**Closed**

Associated revisions

Revision 15d715da - 12.11.2015 14:40 - Tobias Brunner

curl: Be less strict when considering status codes as errors

For file:// URIs the code is 0 on success. We now do the same libcurl would do with CURLOPT_FAILONERROR enabled.

Fixes #1203.

Revision e161238e - 12.11.2015 14:40 - Tobias Brunner

revocation: Allow CRLs to be encoded in PEM format

Since the textual representation for a CRL is now standardized in RFC 7468 one could argue that we should accept that too, even though RFC 5280 explicitly demands CRLs fetched via HTTP/FTP to be in DER format. But in particular for file URIs enforcing that seems inconvenient.

Fixes #1203.

History

#1 - 11.11.2015 15:34 - Tobias Brunner

- Tracker changed from Issue to Bug

- Subject changed from Fetching Crl from files ! to Unable to fetch CRL from files with the curl plugin (or in PEM format)

- Status changed from New to Feedback

- Strongswan must be built with files pluging or this plugin must be installed in case of repo installation;

While this should work with the *curl* plugin too (as long as libcurl was built with --enable-file), I was able to confirm that it doesn't. This is apparently broken since we also return a response received when the status code otherwise would indicate an error. That is, we disable CURLOPT_FAILONERROR but manually check for a result code that indicates and error (basically if it's not in the 200s, which indicates a successful response for HTTP and FTP). The problem is that the result code for successfully fetched file:// URIs is 0. I pushed a commit to the *1203-crl-pem* branch that fixes this by applying the same restrictions libcurl uses when CURLOPT_FAILONERROR is enabled (i.e. codes >= 400 are considered errors).

- files plugin must be specified at load parameter in stronswan.conf;

That depends on your configuration and how you built strongSwan. If you run make clean after changing the configure options newly enabled plugins should get loaded automatically.

- files plugin must be specified before curl plugin if there is, at stronswan.conf;

Only if you want to use it while you have the curl plugin loaded too. With the modular configuration the priority of a specific plugin can also be changed in the respective config file.

- each CA certificate: for example Root and Intermediate certificate to be specified as cacert parameter at "ca" section in ipsec.conf;
- each Crl have to be specified trhough crluri parameter at "ca" section in ipsec.conf;

Yes, if you use file:// URIs that's necessary (otherwise you could embed the URIs in the certificates) but only for the CA that actually issued certificates you want to check. So if you have the intermediate CA installed and only want to check the certificates issued by that certificate (and not the intermediate CA itself) you don't need to configure anything for the root CA - unless, that certificate is in a non-standard location too.

- all necessary Crls must be in DER format.

That's because, by definition, CRLs fetched from HTTP or FTP servers must be encoded in DER format (RFC 5280, RFC 2585). Therefore, the *revocation* plugin assumes that's true for all the CRLs fetched from URIs, including file:// URIs. With the textual encoding of CRLs now standardized (RFC 7468) one might argue that this format (generally called PEM) is now valid too for CRLs fetched from URIs. However, it is not really standardized (neihter are file:// URIs for CRLs for that matter). Anyway, the second patch in the *1203-crl-pem* also allows PEM encoded CRLs.

So, I offer to dev team to make Crl fetching from file easier by adding parameter, for example, "crl" to ipsec.conf where path to Crl have to be put and handle Crl fetching from non-default location as if it would be at default location and in Pem format and without curl or files plugins.

You could also just put symlinks in ipsec.d/crls.

As I saw that Crls located at default location is fetched from file without plugings (at least without files plugin) and in Pem format as well.

Yes, the files in ipsec.d/crls are processed slightly differently.

#2 - 11.11.2015 15:44 - Alex Brew

> As I saw that Crls located at default location is fetched from file without plugings (at least without files plugin) and in Pem format as well.

> Yes, the files in ipsec.d/crls are processed slightly differently.

I suggest to add some parameter for example named "crl" to ipsec.conf where /no-default path/CRLs will be specified that will be processed exactly in the same way as placed at ipsec.d/crls
If this new parameter is an empty or absence, that is default location will be proceeded.
It is aditional wat to existing crluri and crul/files plug-ins way.

#3 - 11.11.2015 15:50 - Tobias Brunner

> As I saw that Crls located at default location is fetched from file without plugings (at least without files plugin) and in Pem format as well.

> Yes, the files in ipsec.d/crls are processed slightly differently.

> I suggest to add some parameter for example named "crl" to ipsec.conf where /no-default path/CRLs will be specified that will be processed exactly in the same way as placed at ipsec.d/crls

Adding a new configuration option that's named so similar to the current option and basically does the same thing is not only confusing but unnecessary. The ipsec.conf configuration backend is legacy anyway (replaced by swanctl.conf/vici).

#4 - 12.11.2015 14:41 - Tobias Brunner

- Category set to libstrongswan

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Target version set to 5.3.4

- Resolution set to Fixed

#5 - 12.04.2018 11:04 - Tobias Brunner

- Related to Issue #2628: "crl fetched successfully but parsing failed" when use CRL added