Audacious - OLD, PLEASE USE GITHUB DISCUSSIONS/ISSUES - Bug #343

Scrobbler refuses last.fm certificate if built with GnuTLS

September 05, 2013 23:05 - Luís Picciochi

Status:	Closed	**Start date:**	September 05, 2013
Priority:	Major	**Due date:**	
Assignee:	Luís Picciochi	**% Done:**	100%
Category:	plugins/scrobbler2	**Estimated time:**	0.00 hour
Target version:			
Affects version:			

Description

So, it appears that last.fm has updated its https certificate.
Until distributions update their recognised CAs (http://packages.debian.org/ca-certificates ?), the scrobbler is unable to connect, as the certificate is deemed invalid.
At least Debian testing is suffering from this.

I haven't chosen a solution yet. Possibilities thought of thus far:

- Allow the user to say he doesn't care if the certificate is invalid, and connect anyway.
  - This is possibly the worst solution. The scrobbling URL is not configurable, and so we only connect to last.fm's https address. If the certificate is untrusted, a connection to that address should never established.
- Allow the user to select whether to connect using https or http.
- Allow the user to select whether to connect using https, with possibility of fallback to http, in case the https connection is not possible.

Any of these is sub-optimal, as using plain http leaves the user subject to replay attacks if his traffic is sniffed.

The best solution would be if the certificate was good and recognised by the distro(s).
It might be necessary to investigate this further with last.fm and/or to annoy the distros' packagers of CA certificates for this to be correctly addressed.

```
$ wget  https://last.fm
--2013-09-05 22:04:53--  https://last.fm/
Resolving last.fm (last.fm)... 195.24.232.203
Connecting to last.fm (last.fm)|195.24.232.203|:443... connected.
ERROR: The certificate of `last.fm' is not trusted.
ERROR: The certificate of `last.fm' hasn't got a known issuer.

$ openssl s_client -showcerts -connect last.fm:443
CONNECTED(00000003)
depth=0 OU = Domain Control Validated, CN = *.last.fm
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 OU = Domain Control Validated, CN = *.last.fm
verify error:num=27:certificate not trusted
verify return:1
depth=0 OU = Domain Control Validated, CN = *.last.fm
verify error:num=21:unable to verify the first certificate
verify return:1
---
(...)
---
Server certificate
subject=/OU=Domain Control Validated/CN=*.last.fm
issuer=/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Domain Validation CA - G2
---
(...)
    Verify return code: 21 (unable to verify the first certificate)
```

Related issues:			
Has duplicate Audacious - OLD, PLEASE USE GITHUB DISCUSSIONS/ISSUES - Bug #34...	**Rejected**	**September 12, 2013**	

History

#1 - September 05, 2013 23:35 - Luís Picciochi

Disregard the previous URLs.

They should be:

```
$ wget https://ws.audioscrobbler.com/2.0/
--2013-09-05 22:32:56--  https://ws.audioscrobbler.com/2.0/
Resolving ws.audioscrobbler.com (ws.audioscrobbler.com)... 195.24.232.205
Connecting to ws.audioscrobbler.com (ws.audioscrobbler.com)|195.24.232.205|:443... connected.
ERROR: The certificate of `ws.audioscrobbler.com' is not trusted.
ERROR: The certificate of `ws.audioscrobbler.com' hasn't got a known issuer.

$ openssl s_client -showcerts -connect ws.audioscrobbler.com:443
CONNECTED(00000003)
depth=2 C = BE, O = GlobalSign nv-sa, OU = Root CA, CN = GlobalSign Root CA
verify error:num=19:self signed certificate in certificate chain
verify return:0
---
Certificate chain
 0 s:/OU=Domain Control Validated/CN=*.audioscrobbler.com
   i:/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Domain Validation CA - G2
(...)
 1 s:/C=BE/O=GlobalSign nv-sa/OU=Root CA/CN=GlobalSign Root CA
   i:/C=BE/O=GlobalSign nv-sa/OU=Root CA/CN=GlobalSign Root CA
(...)
 2 s:/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Domain Validation CA - G2
   i:/C=BE/O=GlobalSign nv-sa/OU=Root CA/CN=GlobalSign Root CA
(...)
Server certificate
subject=/OU=Domain Control Validated/CN=*.audioscrobbler.com
issuer=/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Domain Validation CA - G2
(...)
    Verify return code: 19 (self signed certificate in certificate chain)
```

#2 - September 08, 2013 08:09 - Ruei-Yuan Lu

Currently I built the scrobbler plugin with libcurl4-openssl-dev, instead of libcurl4-gnutls-dev, to avoid this problem.

It works on my Debian Wheezy machine. :)

#3 - September 12, 2013 23:47 - Luís Picciochi

Thanks, Ruey-Yuan.

After investigating this, it seems that the issue may be related with the order the certificates are sent by last.fm.
OpenSSL seems to be more resilient to server (mis?)configurations. After checking if it really solves this issue, a strong dependency on OpenSSL to avoid compiling against GnuTLS may solve this.

Relating to the above openssl command, if CApath is given on the command line, OpenSSL will validate the certificate by looking at the installed CA certs:

```
$ openssl s_client -connect ws.audioscrobbler.com:443 -CApath /etc/ssl/certs/
(...)
    Verify return code: 0 (ok)
```

Doing the same with GnuTLS will not:

```
$ gnutls-cli -p 443 ws.audioscrobbler.com --x509cafile /etc/ssl/certs/ca-certificates.crt
Processed 159 CA certificate(s).
Resolving 'ws.audioscrobbler.com'...
Connecting to '195.24.232.205:443'...
*** Verifying server certificate failed...
*** Fatal error: Error in the certificate.
*** Handshake has failed
GnuTLS error: Error in the certificate.
```

...which may be related to this:
gnutls is tolerant and if the correct chain is provided
in the front of the list then it will verify the chain and not complain.
The problem is if there is no proper chain e.g if certificates are
thrown in a random order.
From https://lists.gnu.org/archive/html/help-gnutls/2012-03/msg00038.html

But I'll need further confirmation on this, to get rid of any biases.

#4 - September 14, 2013 00:40 - John Lindgren

- Subject changed from Scrobbler doesn't scrobble when the last.fm certificate is not recognised to Scrobbler refuses last.fm certificate if built with GnuTLS

#5 - September 15, 2013 00:02 - John Lindgren

Trying to load https://last.fm in Firefox on Windows 7 also complains about a bad certificate. I've notified last.fm of the problem.
http://www.last.fm/forum/21713/_/2215292

#6 - September 16, 2013 23:25 - Luís Picciochi

I couldn't reproduce that with an up to date Firefox (23.0.1) and Windows 7 (64-bit) with all updates installed.
Did you try with all updates?

Anyway, the address in question is ws.audioscrobbler.com, not last.fm. Can you reproduce that on Windows with ws.audioscrobbler.com?

#7 - September 19, 2013 04:52 - John Lindgren

I just now updated Firefox to 24.0 (it was 23.0.1) and that fixed the warning on https://last.fm. Neither 23.0.1 nor 24.0 had a problem with https://ws.audioscrobbler.com.

I hate these problems where none of the symptoms make any sense ...

#8 - September 19, 2013 23:08 - Luís Picciochi

I'll try to look at this with some more time during the next weekend. No promises as usual, though.

John: on #321 you said that you also see this problem on Windows, with OpenSSL. Does that still happen? Windows updates frequently update certificates. Some needed certificate could been missing (?) but now isn't, coincidentally with you updating Firefox.

This is what we know now:
Linux:

- scrobbler built with libcurl-gnutls, doesn't recognise the certificate.
- scrobbler built with libcurl-openssl, trusting Ruei-Yua's comment (#343-2), recognises the certificate

Windows:

- scrobbler built with libcurl-openssl, doesn't recognise the certificate.

This is starting to look more and more a last.fm-side problem.

#9 - September 25, 2013 22:42 - Luís Picciochi

Here are the results from compiling and using the scrobbler on a Debian testing machine, with all updates as of when I performed the tests (Sep 21st, 2013):

libcurl4-gnutls-dev 7.32.0-1:

```
scrobbler_communication.c:151 [send_message_to_lastfm]: Could not communicate with last.fm: Peer certificate c
annot be authenticated with given CA certificates.
```

libcurl4-nss-dev 7.32.0-1:

```
scrobbler_communication.c:151 [send_message_to_lastfm]: Could not communicate with last.fm: Problem with the S
SL CA cert (path? access rights?).
```

libcurl4-openssl-dev 7.32.0-1:
Everything works.

I also tested changing the URL to https://google.com and the connection was well established with both GnuTLS and OpenSSL. Obviously, Google didn't like the subsequent requests, but it's cert was recognised, that's all.
Using the NSS backend gave the same message as before.

This is leading me to conclude that:

- The last.fm certificate is not OK;
- NSS support is not well configured on my machine. Apparently some additional configuration is needed to build a certificate DB, which could be built by the distro[1][2] but for some reason it isn't. It makes no sense to force users/installers to do this kind of magic just to scrobble from Audacious.

1 - http://curl.haxx.se/docs/sslcerts.html (see Peer SSL Verification with NSS)
2 - http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=537866

#10 - September 27, 2013 01:44 - John Lindgren

I still get this on Windows:

```
scrobbler_communication.c:151 [send_message_to_lastfm]: Could not communicate with last.fm: Peer certificate c
annot be authenticated with given CA certificates.
```

#11 - September 27, 2013 22:49 - Luís Picciochi

I have finally received a confirmation from last.fm that the issue is on their side and that they are working to solve it.

Nevertheless, please leave this issue open until the problem is definitely solved.

#12 - September 28, 2013 00:29 - John Lindgren

Luís Picciochi wrote:

> Nevertheless, please leave this issue open until the problem is definitely solved.

Sure.

#13 - October 06, 2013 16:59 - Виктор Пономарёв

Luís, what is known about the correct certificate?

#14 - October 08, 2013 21:14 - Luís Picciochi

I still have no answer from last.fm.

However, yesterday I updated my wget installation, and that came with a dependency on libgnutls28. The previous version was libgnutls26.
The libgnutls26 is version 2.12.23-7, libgnutls28 is 3.2.4-4.

wget is now able to connect to https://ws.audioscrobbler.com , although it gets a 400 error subsequently (but that's not an issue):

```
$ wget https://ws.audioscrobbler.com/2.0/
--2013-10-08 20:02:34--  https://ws.audioscrobbler.com/2.0/
Resolving ws.audioscrobbler.com (ws.audioscrobbler.com)... 195.24.233.55
Connecting to ws.audioscrobbler.com (ws.audioscrobbler.com)|195.24.233.55|:443... connected.
HTTP request sent, awaiting response... 400 Bad Request
2013-10-08 20:02:36 ERROR 400: Bad Request.
$
```

gnutls-bin now also depends on libgnutls28:

```
$ gnutls-cli -p 443 ws.audioscrobbler.com --x509cafile /etc/ssl/certs/ca-certificates.crt
Processed 164 CA certificate(s).
Resolving 'ws.audioscrobbler.com'...
Connecting to '195.24.233.55:443'...

- Certificate type: X.509
- Got a certificate list of 3 certificates.
- Certificate[0] info:
(...)
- Status: The certificate is trusted.
(...)
- Handshake was completed
```

This is leading me to think that quite likely, libgnutls28 (v3.2) is capable of dealing with last.fm's apparently crapped-up certificates. I'm planning to test this further by compiling libcurl against this more recent libgnutls, and see how the scrobbler goes. I'll probably do this over the weekend.

If there's anyone on the audience with more free time than me to do this, feel free to reply with your experience.

#15 - October 15, 2013 00:42 - Luís Picciochi

I just tested the scrobbler with libcurl 7.33.0, which was compiled against GnuTLS 3.2.4.
The scrobbler was able to contact last.fm, and submitted the most recent tracks. Due to a restriction on last.fm's side, older plays were lost. I could only submit tracks played on the last week. The others were at least 3 weeks old, and last.fm happily discarded them.

The solution is then to enforce to build against libcurl, which has to have been built either against libopenssl, or against libgnutls >=3.2.4 (this might be trickier than it seems).

jlindgren: when you tested on Windows, what was libcurl built against? libcurl? libopenssl? Which version?

I'll leave this here so it gets noticed:
Users will lose their oldest scrobbles due to this issue. If users want to re-scrobble their tracks, they should make a backup of ~/.config/audacious/scrobbler.log before upgrading libgnutls and prepare to re-scrobble them after this is solved. The backed-up scrobbler.log can be opened with any text editor.

#16 - October 15, 2013 00:44 - Luís Picciochi

Of course, that should read: what was libcurl built against? **libgnutls**? libopenssl?

#17 - October 16, 2013 05:24 - John Lindgren

I am using OpenSSL 1.0.1e on Windows. The first problem was that OpenSSL didn't know where to look for CA certificates. After copying some certificates from my Linux partition, I can connect to google.com:443 successfully, but last.fm:443 is giving me the same output as in the original bug description:

```
depth=0 OU = Domain Control Validated, CN = *.last.fm
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 OU = Domain Control Validated, CN = *.last.fm
verify error:num=27:certificate not trusted
verify return:1
depth=0 OU = Domain Control Validated, CN = *.last.fm
verify error:num=21:unable to verify the first certificate
verify return:1
```

Edit: I get the same output when I run openssl from the command line in Arch Linux, but in spite of that, the scrobbler can connect. So maybe libcurl+OpenSSL is more tolerant than OpenSSL on its own. I will try some more tests on Windows when I can find the time.

#18 - October 16, 2013 10:17 - Luís Picciochi

Please don't test against last.fm:443 but ws.audioscrobbler.com:443 .

#19 - October 20, 2013 03:21 - Bob Bib

Luís Picciochi wrote:

> I still have no answer from last.fm.

Have you (or anyone else) tried to contact them one more time?

> Due to a restriction on last.fm's side, older plays were lost. I could only submit tracks played on the last week. The others were at least 3 weeks old, and last.fm happily discarded them.
> ...
> **If users want to re-scrobble their tracks, they should make a backup of <config> before upgrading libgnutls and prepare to re-scrobble them after this is solved**

And this looks like separate issue. Do you have any more info on it?

#20 - October 23, 2013 00:48 - Luís Picciochi

I still have no idea on how to portably ensure libcurl was built against gnutls >= 3.2.4. We could check libcurl's version string, but that seems too fragile for the long term. Suggestions are welcome.

Bob Bib wrote:

> Luís Picciochi wrote:
>
> > I still have no answer from last.fm.
>
> Have you (or anyone else) tried to contact them one more time?

I was able to communicate with a last.fm person again today. There's still no progress on their side. The issue is still "in the backlog".

> Due to a restriction on last.fm's side, older plays were lost. I could only submit tracks played on the last week. The others were at least 3 weeks old, and last.fm happily discarded them.
> ...
> **If users want to re-scrobble their tracks, they should make a backup of <config> before upgrading libgnutls and prepare to re-scrobble them after this is solved**

> And this looks like separate issue. Do you have any more info on it?

Yes and no.
I got confirmation from them that scrobbles older than 2 weeks are bluntly discarded by last.fm.

The Audacious scrobbler implements their API quite strictly, so where it says:

http://www.last.fm/api/scrobbling wrote:

> Lfm error codes that indicate a scrobble request should be retried are:
>
> - **11.** Service Offline - This service is temporarily offline, try again later.
> - **16.** The service is temporarily unavailable, please try again.
>
> Additionally this lfm error code indicates that the client should reauthenticate to get a new session key before retrying the request:
>
> - **9.** Invalid session key - Please re-authenticate
>
> All other error codes indicate the scrobble request was incorrectly formed in some way and should not be retried.

I have interpreted this as to only retry attempts that got those errors. last.fm returns an "OK" status for discarded tracks, so the scrobbler happily goes on with that and doesn't look back.
A workaround can be implemented to keep retrying refused, old tracks. I don't like this solution as it goes against last.fm's spec, but I agree that this is better than losing scrobbles. Once again, I'll try to implement that over the weekend.

#21 - October 23, 2013 02:22 - Bob Bib

Luís Picciochi wrote:

> I got confirmation from them that scrobbles older than 2 weeks are bluntly discarded by last.fm.
>
> The Audacious scrobbler implements their API quite strictly, so where it says:
> ...

I just wonder if it is an old bad behavior of Last.fm or a new "bug feature";
if it's new, it obviously can be not reflected in documentation...

#22 - October 24, 2013 00:02 - Luís Picciochi

Bob Bib wrote:

> I just wonder if it is an old bad behavior of Last.fm or a new "bug feature";
> if it's new, it obviously can be not reflected in documentation...

Last.fm has always had a threshold for dropping old scrobbles, and they always documented it. If that threshold was reduced to 2 weeks or 2 days, it's indifferent for the correctness of the specification & implementations.

I'm not seeing a clean way out of this until either last.fm fix their certificates and/or libcurl packagers increase their dependency on libgnutls to libgnutls28.

Until then, I'll probably end up implementing a dirty, version string-based hack to prevent audacious to compile against libcurl with libgnutls < 28.

#23 - October 24, 2013 00:17 - John Lindgren

Luís Picciochi wrote:

> Until then, I'll probably end up implementing a dirty, version string-based hack to prevent audacious to compile against libcurl with libgnutls < 28.

I don't think it's necessary to add a compile-time check, especially since GnuTLS isn't even a direct dependency. The issue should be documented, though. If you email me a few sentences summarizing the issue, I'll add them to http://audacious-media-player.org/problems.

#24 - October 28, 2013 02:28 - Luís Picciochi

I started working on a quick fix so no scrobbles are lost. See http://redmine.audacious-media-player.org/issues/260#note-1

Once this is commited, users will have to update their Audacious **before** last.fm fixes their servers. If not, they will still have to back-up their scrobbler.log file (which I recommend doing ASAP anyway).

jlindgren: I'll hand you a description of these problems + workarounds once I have the code ready for integrating with the main branch (hopefully tomorrow or on Wednesday).

#25 - October 29, 2013 09:04 - Виктор Пономарёв

Luís, whether correctly I understand that I will have to update a Audacious with your decision before there will be a communication with last.fm?

#26 - October 30, 2013 01:43 - John Lindgren

Linking back to http://audacious-media-player.org/news/24-scrobbler-issue for reference.

#27 - November 16, 2013 13:40 - Виктор Пономарёв

What progress now?

#28 - December 10, 2013 16:40 - Jon Hallier

Hi from Last.hq,

Sorry this has taken so long, but we've finally addressed the ordering of the certificates and this problem should now be resolved. If it isn't, please let me know (best to send a pm to my last.fm account) and I'll ask the team to take another look.

Cheers,
-Jon

#29 - December 13, 2013 23:35 - Luís Picciochi

Well, *better late than never*. Thanks for the update, Jon.

I confirm that at least some communication is possible with audacious 3.4.1 (with libcurl built against an old libgnutls). I didn't test all of the interactions yet (including scrobbling), though.

Can someone confirm if the Windows version is also working?

#30 - December 14, 2013 20:24 - John Lindgren

I was looking into the Windows version a while back, and it seems that OpenSSL doesn't know how to access the client-side certificates that Windows provides. There are various bits of code posted online that will fetch the certificates and feed them into OpenSSL, but I haven't implemented such a workaround in Audacious (nor will I have time in the near future).

#31 - December 15, 2013 17:14 - Виктор Пономарёв

Audacious 3.4.2 communicate with Last.fm (I checked by logging into another profile).

Will I lose my listening when I'm connected to Last.fm into base profile?

#32 - December 15, 2013 17:23 - Виктор Пономарёв

Виктор Пономарёв wrote:

> Audacious 3.4.2 communicate with Last.fm (I checked by logging into another profile).
>
> Will I lose my listening when I'm connected to Last.fm into base profile?

I meant Linux version.

#33 - December 15, 2013 17:37 - Luís Picciochi

Copy the ~/.config/audacious/scrobbler.log file to a backup location.

Then start Audacious configured with your profile. Look at your last.fm profile to see all your old plays start appearing.

#34 - December 16, 2013 04:49 - Виктор Пономарёв

- File scrobbler.log added

Something went wrong.

I had 12 590 plays on Last.fm.

scrobbler.log contains 3540 songs.

1. When I listen the song, list of plays loaded on the server. The first batch of sent contained line 3517 - 3540. This can be seen on page http://www.lastfm.ru/user/v_pv/tracks?view=compact&page=58 . First song is "Kick Bong – Voice Of Resurrection", second song is "The Gentle Revolution – Stealth and Cunning", third song is "Hol Baumann – Breathe" etc. The final song is "Cell – Under Your Mind".
2. The second batch of sent contained unknown positions. I don't know, from what place of the file tracks are loaded. There was a set of repetitions of one track (for example, http://www.lastfm.ru/user/v_pv).
3. There was a loading of 3402 tracks from 3540. After that Last.fm displayed listenings, but didn't fix it.

Such affairs.

#35 - December 16, 2013 22:57 - Luís Picciochi

You didn't happen to start audacious with -V and save the output to a file, did you?

#36 - December 17, 2013 06:25 - Виктор Пономарёв

Luís Picciochi wrote:

> You didn't happen to start audacious with -V and save the output to a file, did you?

Yes, of course.

I plan to clear the list of listenings and reload scrobbler.log. Please remind me the command with -V attribute and output parameter.

#37 - December 20, 2013 19:36 - Виктор Пономарёв

- File log1.txt.zip added

I cleared the list of listenings. I wanted to load the list anew. 699 compositions were loaded.

#38 - December 20, 2013 20:39 - Luís Picciochi

- File deleted (log1.txt.zip)

#39 - December 20, 2013 20:43 - Luís Picciochi

I deleted the log from this issue because it contained your full submissions, including signature - this can allow others to re-scrobble those plays. I should remove that output from the scrobbler's debug mode.

Anyway, thanks for all the input. I'll try to look into this on Sunday. These are busy days around here. :-)

#40 - January 11, 2014 20:26 - John Lindgren

Can we close this since the certificate ordering problem is resolved? Further support questions can be asked and answered on the forums.

#41 - January 19, 2014 02:16 - John Lindgren

- Status changed from New to Closed

- % Done changed from 0 to 100

Closing.

Files

scrobbler.log	232 KB	December 16, 2013	Виктор Пономарёв