Closed · Issue created 2 years ago by **Damian Poddebniak**

(CVE-2020-24661) Invalid certificates not checked against locally pinned certificates when GCR support not available

If there is no read-write PKCS#11 store accessible by GCR (e.g. gnome-keyring-daemon is not installed, the gnome-keyring user PKCS#11 store is not installed or enabled, or gnome-keyring has dropped support for it, again), and an exception for an invalid TLS certificate has previously been allowed by the user for a specific server identity (e.g. the host name/IP address configured for the service), then subsequent connections to the same server identity will be accepted without comparing the certificate presented by the server with the certificate that was originally presented and pinned.

This allows e.g. MITM attacks against connections with the same configured identity when using invalid certificates.

This can be mitigated by any of: a) ensuring your system is correctly configured WRT PKCS#11 stores, b) not using invalid certificates (including self-signed certificates), c) not creating exceptions for invalid certificates.

Original description:

Bug Summary

Geary accepts self-signed X.509 certificates when doing STARTTLS (and probably also implicit TLS). This allows a Meddler-in-the-Middle (MitM) to steal emails and user credentials.

Your installation

- Geary version: geary-3.34.2 (NixOS)
- Installation method: nix-env -i
- Desktop environment: KDE
- Operating system and version: https://channels.nixos.org/nixos-20.03/latest-nixos-x86_64-linux.ova
- Email provider: not important

Steps to reproduce

1. Setup a local mailserver with an "invalid" X.509 certificate, i.e. self-signed, one where the root-CA is not trusted by the operating system, etc. (I used mkcert, https://github.com/FiloSottile/mkcert)
2. Try to connect Geary to that mail server and observe that no warning is displayed.

What did you expect to happen?

Geary should under no circumstances just proceed with the connection. It must issue a warning and obtain user permission to do so. IMHO Thunderbird is a good example how to do it properly.

Relevant logs and/or screenshots

Edited 2 years ago by Michael Catanzaro

Drag your designs here or click to upload.

Tasks 0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items 0

Related merge requests 3

- Fix invalid certificate pinning when GCR support is unavailable
  !529
- Merge branch 'mjog/866-self-signed-certificates' into 'gnome-3-36'
  !557 · 3.36.3
- Self signed certificates unit tests
  !559

When these merge requests are accepted, this issue will be closed automatically.

Activity

Damian Poddebniak @duesee1 · 2 years ago · Author

Just in case: does anybody see this issue? Asking because GitLab tells me that "People without permission will never get a notification".

Damian Poddebniak changed the description 2 years ago

Michael Catanzaro @mcatanzaro · 2 years ago · Developer

@mjog, have you seen this?

Damian Poddebniak @duesee1 · 2 years ago · Author

Okay, I wanted to provide more information about the used certificates and my config and was not able to reproduce the issue on my second laptop at first. The reason seems to be that Geary only accepts bad certificates (unknown root, cn/san mismatch, self-signed), if the user accepted the security prompt ("Always trust this server") in the past.

I did a fresh setup (also deleted all Geary config folders) with a valid certificate "A" (Let's Encrypt.) Then, I exchanged it to an invalid certificate "B" and was prompted with the security dialog, which I *accepted*. This is good. However, when I change the certificate again to an unrelated self-signed certificate "C", Geary automatically accepts this, too.

I tried to find any config saying "accept all certificates" or something like that, but was not able to find one.

Edited by Damian Poddebniak 2 years ago

Michael Catanzaro @mcatanzaro · 2 years ago · Developer

In other words: trusting one particular certificate creates a permanent trust exception for all certificates.

I recommend Geary not offer to trust untrusted certificates at all. It's 2020 and nobody is going to be using untrusted certificates on a production mail server.

Damian Poddebniak @duesee1 · 2 years ago · Author

Additional note: accepting the bad certificate in IMAP also seems to create the trust exception for SMTP.

Michael Gratton @mjog · 2 years ago · Developer

Do your IMAP and SMTP services have the same host name? If so then this is intentional - certs are host-specific, not (host:service)-specific.

Damian Poddebniak @duesee1 · 2 years ago · Author

Yes, both used the same domain.

Please register or sign in to reply

Michael Gratton @mjog · 2 years ago · Developer

Geary was previously using GCR for this exclusively, but around 3.30/3.32 GCR (or maybe gnome-keyring-daemon?) changes broke it for a cycle or two. When Geary detects that situation, it works around it with a custom cert hash store. So the problem could be in any of those places.

@duesee1, could you open the Geary Inspector shortly after app launch (`Alt+I`) and search for `GCR`, then post the matching log entries? They shouldn't be confidential.

@mcatanzaro AFAICT there's still some call for it, even Proton Mail's bridge uses self-signed certs: https://protonmail.com/bridge/thunderbird#5 :(

Michael Gratton @mjog · 2 years ago · Developer

tbh, I'd rather like to implement cert pinning, which basically amounts to the same thing in the end.

Damian Poddebniak @duesee1 · 2 years ago · Author

```
  [deb] 15:07:31.0609 Gcr: starting initialize of registered modules
 *[wrn] 15:07:31.0609 GLib-GObject: value "-1" of type 'gint' is invalid or out of range for property 'position' of type '
  [deb] 15:07:31.0610 Gcr: completed initialize of registered modules
```

```
[deb] 15:07:31.0610 Gcr: trust store uri is: (null)
[deb] 15:07:31.0610 Gcr: trust lookup uris are: pkcs11:library-description=PKCS%2311%20Kit%20Trust%20Module
[deb] 15:07:31.0610 geary: application-certificate-manager.vala:71: GCR slot URIs found: false
```

Michael Gratton @mjog · 2 years ago — Developer

It looks like you don't have gnome-keyring-daemon or the gnome-keyring PKCS#11 module installed, it is misconfigured, or the PKCS#11 store that it provides has been removed upstream by gnome-keyring again (see gnome-keyring#20 (closed)) or by the downstream distro. These are all packaging or upstream bugs, fwiw.

Assuming gcr#6 hasn't actually been fixed or some other change there or in gnome-keyring has broken things again, for this to work properly, `find / -name gnome-keyring-pkcs11.so` has to report something. If not, work out how to get that file installed on your system such that gnome-keyring-daemon can load it and this should start working properly.

Edited by Michael Gratton 2 years ago

Michael Gratton @mjog · 2 years ago — Developer

@dueseel , one other followup, what does `ls ~/.local/share/geary/pinned-certs/` show?

Michael Gratton @mjog · 2 years ago — Developer

@dueseel I've pushed a potential fix to !529 (merged), can you please verify that addresses the issue for you? Thanks!

Damian Poddebniak @dueseel · 2 years ago — Author

Sorry, I was on vacation and didn't followed the discussion very closely. I am not familiar with Geary and afraid that I will not have the time to take a deep dive into Geary and verify if everything is fine now. I can clone and build Geary and see if the issue goes away, but you can test this a lot more rigorously than I can for sure. Is there anything specific I can still provide to you? Do you still need the output of `ls ~/.local/share/geary/pinned-certs/` ? If so, I will provide it tomorrow.

Michael Gratton @mjog · 2 years ago — Developer

@dueseel apologies for the late reply. No I don't think I need that dir listing. I'm happy with the fix, but if you could try building the branch in the MR from git `mjog/866-self-signed-certificates` and let me know if it fixes the cases you are concerned about, that would be good.

Please register or sign in to reply

Michael Catanzaro @mcatanzaro · 2 years ago — Developer

> tbh, I'd rather like to implement cert pinning, which basically amounts to the same thing in the end.

OK, so you implemented "Always trust this server" but you did it without certificate pinning (which is what users would expect?) and instead just don't check server identity at all when connecting?

Even certificate pinning is a bad idea IMO, because users have no way to choose what to do when the certificate changes, which must happen regularly because certificates expire. But if you must match Thunderbird's behavior for compat reasons, then that's a lot better than not checking the certificate altogether....

Michael Gratton @mjog · 2 years ago — Developer

> OK, so you implemented "Always trust this server" but you did it without certificate pinning (which is what users would expect?) and instead just don't check server identity at all when connecting?

I'm not sure how you came to that conclusion based on what I said, but no, that's not the case. Honest question, why is it that pretty much every core GNOME developer assumes I'm incompetent by default? Is it because I don't program in C?

What actually happens is that a custom GTlsDatabase is used that forwards certificate loading and storage to the system-level PKCS#11 store if available, or if not stores certificates on a per-host-name basis either in memory or on disk. Existing GLib machinery is used to handle verification, and this is set as the database for GTlsClientConnections (at the appropriate time) for outgoing connections.

Michael Catanzaro @mcatanzaro · 2 years ago — Developer

> I'm not sure how you came to that conclusion based on what I said, but no, that's not the case. Honest question, why is it that pretty much every core GNOME developer assumes I'm incompetent by default? Is it because I don't program in C?

I'm just trying to understand what's happening here. I came to that conclusion based on the reported behavior:

> I did a fresh setup (also deleted all Geary config folders) with a valid certificate "A" (Let's Encrypt.) Then, I exchanged it to an invalid certificate "B" and was prompted with the security dialog, which I *accepted*. This is good. However, when I change the certificate again to an unrelated self-signed certificate "C", Geary automatically accepts this, too.

Clearly, if the report is accurate, then certificate pinning must not be properly implemented. Your description of how the trust store is designed sounds good, though....

Michael Catanzaro @mcatanzaro · 2 years ago — Developer

BTW, since you asked an honest question, I'll give you an honest answer: I'm annoyed when I see bugs like this, but probably less so than you might be thinking; tone rarely conveys well in text. I assume it's just a bug, not incompetence. We all have no shortage of bugs in our code. Certainly I don't assume or accuse you of incompetence.

I also certainly don't consider Vala programmers to be less-skilled than C programmers; you still have to be familiar with C anyway to debug crashes in generated code that's much harder to read than human-written C, plus also a bindings expert when things go wrong with the bindings....

Michael Gratton @mjog · 2 years ago — Developer

You may not have meant to make that assumption, but that's certainly what you did. It's simply not possible for someone to implement self-signed certificate handling in the way you describe unless they were either ignorant of or just not cared about the issues around certificate handling and why they are important, i.e. by-definition incompetent. That is exactly what you assumed I had done: `OK, so you implemented…` , and you did so without looking into it yourself first, asking to clarify what I was talking about, or asking to clarify how I had actually implemented it -- you just made the assumption.

I asked because assuming incompetence like this is the common case when I am interacting with many GLib, GTK, etc developers both in GitLab and elsewhere. I have been told over the last few years that variously "your (app design,dev requirements,end-user experience expectations) are (stupid,wrong)" etc., I've had trivial library use and CS101-level concepts explained to me as if I wasn't aware of them, and so on. As this issue clearly shows I am by all means imperfect. However the constant assumption that I am incompetent has finally in the last month or two put me off trying to contribute to those projects and GNOME in general, and quite frankly, copping that here makes me want to stop working on Geary, too.

As an aside, the "communication is lossy on the Internet" argument is entirely bogus. It is possible to communicate on the Internet without coming across as a jerk, it requires however not only not being a jerk in the first place, but also (for those who aren't jerks) going to the effort to not come across as one. Also, since this argument is most often used as a defence by people who actually are jerks to excuse their bad behaviour, it probably is not a great fall-back lest people start thinking that of you, too.

Michael Catanzaro @mcatanzaro · 2 years ago — Developer

> You may not have meant to make that assumption, but that's certainly what you did. It's simply not possible for someone to implement self-signed certificate handling in the way you describe unless they were either ignorant of or just not cared about the issues around certificate handling and why they are important, i.e. by-definition incompetent.

Michael, looking at your merge request, do you disagree that you implemented "Always trust this server" without certificate pinning? Because it sure looks like broken pinning is *exactly* what happened here. I see you tried. Honestly, it's really just a bug. Without quality tests (and almost no GNOME projects have quality tests, including my own), it could happen to anyone. Programming is hard and everyone makes mistakes. We had another certificate verification bug in another GNOME-related project about two months ago that was just as bad. Then we had a disaster in GnuTLS last month because the wrong certificate was used for a security check. And I have yet another certificate verification bug report on my hands right now that I suspect might turn into "d'oh mcatanzaro should not have removed that, turns out that was important." It happens, again and again, to *everyone*. You're not incompetent. (At least, not any more so than everybody else. Humans are bad at programming....)

> That is exactly what you assumed I had done: `OK, so you implemented…` , and you did so without looking into it yourself first, asking to clarify what I was talking about, or asking to clarify how I had actually implemented it -- you just made the assumption.

Well, yes, based on the behavior described by the bug reporter, it seemed like a pretty reasonable assumption. I don't have time to thoroughly investigate every issue myself; fortunately, I don't have to, because GNOME has skilled project maintainers like you to handle them.

> I asked because assuming incompetence like this is the common case when I am interacting with many GLib, GTK, etc developers both in GitLab and elsewhere. I have been told over the last few years that variously "your (app design,dev requirements,end-user experience expectations) are (stupid,wrong)" etc., I've had trivial library use and CS101-level concepts explained to me as if I wasn't aware of them, and so on. As this issue clearly shows I am by all means imperfect. However the constant assumption that I am incompetent has finally in the last month or two put me off trying to contribute to those projects and GNOME in general, and quite frankly, copping that here makes me want to stop working on Geary, too.

I don't have a good response to this. Perhaps it's possible that you're reading a bit much into such comments? Anyway, I can't speak to what happened in your conversations with other people, but in my case, lest I leave any doubt: I'm impressed by your work with Geary. On the rare occasions when I've tried to investigate bugs in the past, I was intimidated by its complexity and never succeeded in

understanding much or accomplishing anything, whereas you're committing fixes on a regular basis. Thank you for maintaining it! Your work is *much* appreciated.

> As an aside, the "communication is lossy on the Internet" argument is entirely bogus. It is possible to communicate on the Internet without coming across as a jerk, it requires however not only not being a jerk in the first place, but also (for those who aren't jerks) going to the effort to not come across as one. Also, since this argument is most often used as a defence by people who actually are jerks to excuse their bad behaviour, it probably is not a great fall-back lest people start thinking that of you, too.

OK... and yet somehow I have a hard time believing we would be arguing here if we were discussing this in person. Humans are generally too friendly. :) Anyway, if you don't like "communication is lossy on the Internet," then at least let's try "assume good intentions," OK?

Michael Gratton @mjog · 2 years ago Developer

> Michael, looking at your merge request, do you disagree that you implemented "Always trust this server" without certificate pinning?

Yes, I do disagree, because it's what I implemented. Clearly implementing pinning without verifying the presented cert matches the pinned one is pretty pointless, but hey I was frustrated and under the pump at the time after an unannounced, downstream-driven change to gnome-keyring broke that part of GCR/GCK API and people were complaining they couldn't log in to their mail server any more after upgrading.

> then at least let's try "assume good intentions," OK?

I do try, but given the amount of push back I get from other platform developers, it's hard to when I get that here as well.

Apologies for jumping down your throat about this.

Edited by Michael Gratton 2 years ago

Michael Catanzaro @mcatanzaro · 2 years ago Developer

> Apologies for jumping down your throat about this.

OK, I hope we're good :)

Please register or sign in to reply

Tobias Mueller @tobiasmue · 2 years ago Developer

> Even certificate pinning is a bad idea IMO, because users have no way to choose what to do when the certificate changes

The idea of pinning the certificate is not directly tied to a specific implementation of a UI or a workflow, right? So unless you are convinced that it is impossible to come up with a sane enough UI, you should not reject the idea itself.

I have an opinion on how that should work, UI and workflow wise, but it may not be compatible with how Geary does things at the moment. It boils down to leading the user to the account setup in case the connection failed due to an invalid certificate (but please please no (modal) popup). There, the parameters of the connection, including the certificate, can be set.

Michael Gratton @mjog · 2 years ago Developer

I'd be interested to hear what you were thinking about that - I've been thinking in the background about how it might work, but don't have any concrete plans yet.

Please register or sign in to reply

Michael Catanzaro changed due date to August 27, 2020 2 years ago

Michael Catanzaro @mcatanzaro · 2 years ago Developer

May 29 + 90 days = Aug. 27 for disclosure (if not fixed before then)

Michael Catanzaro @mcatanzaro · 2 years ago Developer

We're coming up on this date. Any plans to commit the fix in !529 (merged)?

We also need to request a CVE for this issue. I can handle that if nobody else prefers to do so.

Michael Gratton @mjog · 2 years ago Developer

I'll give Damian a couple of days to provide some feedback if possible before landing it.

I've never had to request a CVE, if you can give me a pointer I'll look into it.

Michael Catanzaro @mcatanzaro · 2 years ago Developer

Oh wow, I left this bump comment after you left your other comments here today, but before I read my notifications and noticed your other comments. I wouldn't have pinged here at all had I read my email first. :)

Please register or sign in to reply

Michael Gratton mentioned in commit 0d957559 2 years ago

Michael Gratton mentioned in merge request !529 (merged) 2 years ago

Michael Gratton changed title from **Geary accepts self-signed certificates.** to **Invalid certificates not checked against locally pinned certificates when GCR support not available** 2 years ago

Michael Gratton changed the description 2 years ago

Michael Gratton added 1. Bugs 1. Security Client labels 2 years ago

Damian Poddebniak @duesee1 · 2 years ago Author

Hello all, I don't have any particular feedback. Thank you very much for fixing this!

Michael Gratton @mjog · 2 years ago Developer

Thanks Damian. I'll land this on master now and put out a 3.36.3 with it.

Michael Gratton closed via commit 0d957559 2 years ago

Michael Gratton closed via commit 423a55b0 2 years ago

Michael Gratton changed milestone to %3.36.3 2 years ago

Michael Gratton mentioned in commit 99393b36 2 years ago

Michael Gratton mentioned in merge request !557 (merged) 2 years ago

Michael Gratton mentioned in commit d4e86dc9 2 years ago

Michael Gratton mentioned in merge request !559 (merged) 2 years ago

Damian Poddebniak @duesee1 · 2 years ago Author

Could you make this issue public? This will be useful when registering the CVE.

Michael Gratton made the issue visible to everyone 2 years ago

Michael Gratton @mjog · 2 years ago Developer

Sure thing.

What's the usual process here? Do a release to fix the issue and then get a CVE that points to the release? Or get a CVE and then do a release that points to the CVE?

Michael Catanzaro @mcatanzaro · 2 years ago Developer

Either way is OK, but I prefer the later so that you can reference the CVE ID in the release NEWS. I also prefer to make the issue public before requesting the CVE so that we don't have to submit a second request later to add issue and MR references. (Should be fine; this issue is unlikely to be exploited in the short time between when we make it public and when distros release fixes.)

The best way to request a CVE is to use https://cveform.mitre.org/ and check the box "I have verified that this vulnerability is not in a CNA-covered product." Any one of us can submit the request.

Michael Gratton @mjog · 2 years ago Developer

CVE has been requested, just waiting to hear back with the id.

Michael Gratton @mjog · 2 years ago Developer

CVE assigned: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24661

Getting the releases out now.

Michael Catanzaro changed title from **Invalid certificates not checked against locally pinned certificates when GCR support not available** to **(CVE-2020-24661) Invalid certificates not checked against locally pinned certificates when GCR support not available** 2 years ago

Michael Gratton mentioned in commit 423a55b8 2 years ago

Please register or sign in to reply