(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 sever identity (e.g. the host name/Pb 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.

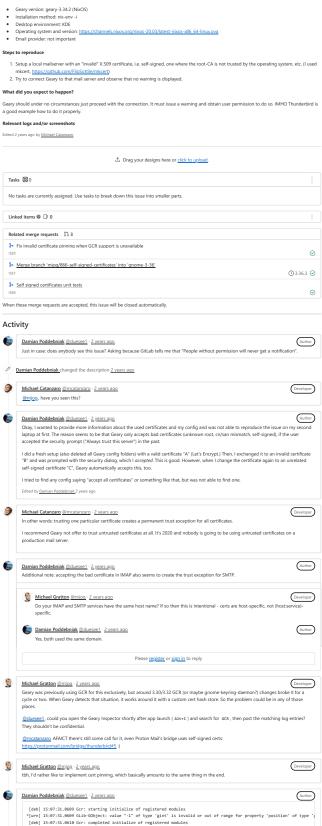
This can be mitigated by any of a) ensuring your system is <u>correctly configured WRT PKCS#11</u> stores, b) not using invalid certificates (including self-signed certificates), c) not creating exceptions for invalid certificates.

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

a good example how to do it properly



[deb] 15:87:21.8618 Gcr: trust store uri is: (null)
[deb] 15:87:21.8618 Gcr: trust lookup uris are: pkcs11:library-description=PKCSX2311X28K1EX20TrustX200T[deb] 15:87:21.8618 geary: application-certificate-amanger-vals:71: GCR slot URIs found: false Michael Gratton @mjog · 2 years ago t looks like you don't have gnome-keyring-daemon or the gnome-keyring PKCS#11 module installed, it is misconfigured, or the PMCS#11 store that it provides has been removed upstream by gnome-keyring again (see gnome-keyring#20 (dosed)) or by the downstream distro. These are all packaging or upstream bugs, fivin. Assuming 0g#6 hasn't actually been fixed or some other change there or in gnome-keyring has broken things again, for this to properly, find / -name grome-keyring-pkcsil.so has to report something. If not, work out how to get that file installed on yor system such that gnome-keyring-daemon can load it and this should start working properly. Michael Gratton @mjog · 2 years ago @duesee1, one other followup, what does 1s ~/.local/share/geary/pinned-certs/ show? Michael Gratton @mjoq - 2 years ago @duesee1 I've pushed a potential fix to 1529 (merged), can you please verify that addresses the issue for you? Thank Damian Poddebniak @duesee1 - 2 years ago 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, buy out an lets this a to more rigorously than I can for sure. Is there anything specific I can still provide to you? Do you still need the output of Is -/.local/share/geary/pinned-certs/? If so, I will provide it tomorow. Michael Gratton @mjog · 2 years ago <u>@duesed_apologies for the late reply.</u> 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 njog/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 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 Even certificate pinning is a bad idea IMO, because users have no way to choose what to do when the certificate changes, which must happer 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 OK, so you implemented "Always trust this server" but you did it without certificate pinning (which is what users would expect?) 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 <u>custom GTIsDatabase</u> 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 andle verification, and this is set as the database for GTIsClientConnections (at the appropriate time) for outgoing conn Michael Catanzaro @mcatanzaro · 2 years ago 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 his, 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 @micaturizaro - 2_versi ago

BTM, 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 t debug crashes in generated code that's much harder to read than human-written C, plus also a bindings expert when things go wro with the bindings Michael Gratton @mjoq · 2 years ago ou may not have meant to make that assumption, but that's certainly what you did. It's simply not possible for someone to imple 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: 0K, sc cerunciar nariumg and why mey are important, i.e. by-deminuor incompetent. That is exactly what you assumed that come. Ox, is you suplemented, 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 Fasceto Destable assuming I have been for the Common that the Common that a micropal control of the Common t 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 jet, 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

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 certificite handling and with they are important, it. by-definition incompetent.

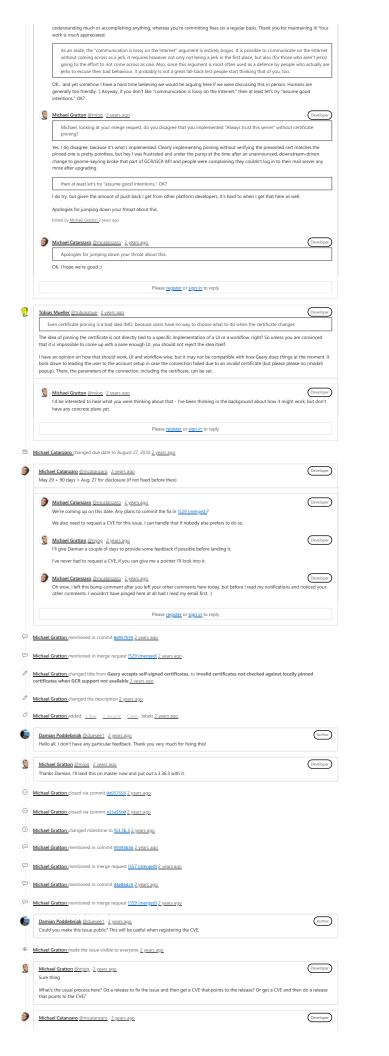
Michael, looking at your mege request, do you disagree that you implemented "Always trust this server" without certificate pinning? Because it sure looks like broken pinning is exortly what happened here. I see you tred. Honestly, list really just a bug. Without quality tests (and almost no GNOME projects have quality tests, including my own, if 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 that Then we had ad disaster in GnuTLS last month because the womon certificate we used for a security device. And It have yet another certificate verification bug report on my hands right now that I suspect might turn into "doh metamazaro should not have removed that turns out that was important." It happens, adia in ad 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 then.

I asked because assuming incompetence like this is the common case when I am interacting with many GLib, GTK, etc developers both in Gitab and elsewhere. I have been told over the last few years that variously 'your lapp design,dev requirements,end-user seperience expectations are (stuplemong)* etc., I've had virtal library use and CS101-level consorts explained to me as I'v 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 fin impressed by your work with Giasy. On the rare cossions when I've that of investigate bugs in the past, I was intimitated by its complexly and never succeeded in



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 factors release flexs.)

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 @micro : 2 years ago

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

Michael Gratton @micro : 2 years ago

CVE assigned: https://cve.mitre.org/https://cve.mitre.o