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

CVE-2020-14928: Response Injection via STARTTLS in SMTP and POP3

We found a STARTTLS issue in Evolution, which affects SMTP and POP3.

When the server responds with its "let's do TLS now message", e.g. `+OK begin TLS\r\n`, Evolution will read any data after the `\r\n` and save it into some internal buffer for later processing. This is problematic, because a MITM attacker can inject arbitrary responses. I havn't tested it to this extent, but I suspect that this is enough to forge an entire new POP3 mailbox.

There is a nice blogpost by Wietse Venema about a "command injection" in postfix (http://www.postfix.org/CVE-2011-0411.html). What we have here is the problem in reverse, i.e. not a command injection, but a "response injection."

Example trace to give an intuition:

```
C: stls
S: +OK begin TLS
   +OK ack future user command // injected response
   +OK ack future pass command // injected response
<--- TLS --->
C: user alice
// here, Evolution interprets the first injected "+OK" response and proceeds...
C: pass password
// here, Evolution interprets the second injected "+OK" response and proceeds...
...
```

An attacker can inject many more responses and (in the worst case) mimic a whole session.

I can also provide a pre-compiled test server to test for the SMTP and POP3 issues.

There are (from my view) three possible fixes: 1) discard any remaining data after stls, 2) shovel the extra data into the TLS layer (where it belongs), and 3) error out as this is clearly a protocol violation.

Edited 2 years ago by Milan Crha

To upload designs, you'll need to enable LFS and have an admin enable hashed storage. More information

Tasks 0

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

Linked items 0

Activity

Milan Crha @mcrha · 2 years ago Maintainer

Thanks for a bug report. If I understand it correctly, then the attacker can pretend whole session, thinking it can guess how the commands will flow, but only until the client sends any data to the server, which should respond with an error, even piled up somewhere at the end of the fake responses, right? I mean the attacker cannot steal anything private, it can only pretend message had been sent (in SMTP) or foist fake messages to the client (in POP).

> Evolution will read any data after the `\r\n` and save it into some internal buffer for later processing.

Do you have any easy reproducer for this, please? I do not understand how SMTP and POP3 can be affected, but not IMAP (nor NNTP). The code is not the same, but it's quite similar and uses the same underlying code. From that I'd guess the problem would be even lower, in glib or glib-networking, whose streams are used here.

Damian Poddebniak @duesee1 · 2 years ago Author

Would a pre-compiled test server work for you? I have not open sourced the server yet, but you should be able to use the provided config files to verify all issues. If so, I can send an email to you with some more explanation.

Milan Crha @mcrha · 2 years ago Maintainer

Precompiled rather not, my environment might not be the same as that yours (I'm pretty sure it's not). I hoped it'll be some kind of a script, because the man-in-the-middle might not need to develop his/her own server to reproduce the problem, right? On the other hand, I agree that exposing fully working exploit may lead to just make it attractive to the attackers.

Damian Poddebniak @duesee1 · 2 years ago Author

Okay, I will work something out. I have an older example to test the issue in IMAP and think it shouldn't be too difficult to adapt it to SMTP and POP3.

Damian Poddebniak @duesee1 · 2 years ago Author

Hey, I figured it is most easy for me to just package a stripped-down version of the server I feel comfortable with to share. (link removed)

Just run `cargo build` and start the server in `target/debug/fake_mail_server`. It listens on ports 110, 25, and 587 by default (see `config.ron`), so you need to arrange that you are allowed to listen on this ports (sudo, set caps, ...) or change them.

You will also need to modify testcases/{smtp,pop3}/B_1.ron as you go -- you will find more explanation in these files.

I used `mkcert -pkcs12` (https://github.com/FiloSottile/mkcert) to create the needed local certificates. Just replace `<container.p12>` with your p12 files. The password with this tool is "changeit" per default.

Edited by Damian Poddebniak 2 years ago

Milan Crha @mcrha · 2 years ago Maintainer

I'm sorry, this seems to be still too complicated. I never ever used anything from what seems natural to you, thus when it ends with something like this:

```
$ target/debug/fake_mail_server
thread '<unnamed>' panicked at 'called `Result::unwrap()` on an `Err` value: Os { code: 13, kind: PermissionDenied, messag
' panicked at 'note: run with `RUST_BACKTRACE=1` environment variable to display a backtrace
called `Result::unwrap()` on an `Err` value: Os { code: 13, kind: PermissionDenied, message: "Permission denied" }', src/r
' panicked at 'called `Result::unwrap()` on an `Err` value: Os { code: 13, kind: PermissionDenied, message: "Permission de
thread 'main' panicked at 'called `Result::unwrap()` on an `Err` value: Any', src/main.rs:85:9
```

Then I'm simply lost. I even do not know what I'm looking for.

Damian Poddebniak @duesee1 · 2 years ago Author

Sorry when I took some things for granted. I packaged this up in the hope that you should do no more than build and run it. What you are seeing is probably a permission issue. Can you change all ports to something over 1000 in the config.ron file and try again?

Edited by Damian Poddebniak 2 years ago

Milan Crha @mcrha · 2 years ago Maintainer

Ah, easy, it was really only about the ports. I thought it requires root permission or something, while I run it only as a regular user. It seems to listen on the port now.

You said I should modify the test cases, but even after opening the files I do not know what I'm supposed to do with them.

Damian Poddebniak @duesee1 · 2 years ago Author

Okay, so let us start with POP3 then. You need to configure Evolution to use your local server. What I did in my setup was to just put "127.0.0.1 mydomain.com" in "/etc/hosts" and take "alice@mydomain.com" as the email address I want to configure. When you changed the ports you also need to tell Evolution which ports :-) You can also test with netcat "nc 127.0.0.1 yourport" to connect to the server and verify that everything works.

Edited by Damian Poddebniak 2 years ago

Damian Poddebniak @duesee1 · 2 years ago Author

If everything works, you should see a colorful trace in the terminal windows where the server is running and see what Evolution is doing. Did you installed a local certificate? Since we are testing TLS, we need to provide a certificate. The easiest solution is to use the mkcert tool I mentioned earlier. Then, just replace `<container.p12>` in the ron files in the testcases folder with the path to your pkcs12 file.

Edited by Damian Poddebniak 2 years ago

Milan Crha @mcrha · 2 years ago Maintainer

I can connect to it, that's easy. I gave it some certs, but it didn't work (code: 587686001, library: "PKCS12 routines", function: "PKCS12_parse", reason: "mac verify failure", file: "crypto/pkcs12/p12_kiss.c", line: 70), so I'm about to generate a new cert.

Damian Poddebniak @duesee1 · 2 years ago Author

You need to provide a certificate and a key. Normally, an attacker does not have the key, but as we are only testing here, we can just assume we had it. The PKCS12 file is a container, which bundles a certificate and a key and secures it with a password. I am not sure why you are seing the message, though. Have you provided a PKCS12 file or just a certificate? Btw, thanks to sticking with it to me.

Edited by Damian Poddebniak 2 years ago

Damian Poddebniak @duesee1 · 2 years ago Author

If you like I can create a PKCS12 file for you. However, then Evolution will complain that the cert is not valid. However, this is not so important for the buffering issue.

Edited by Damian Poddebniak 2 years ago

Milan Crha @mcrha · 2 years ago Maintainer

I made certificates work, that fine. I can connect with both POp and SMTP. What am I looking at now? I see something like this:

```
[2020-06-18 15:07:35.299295042 UTC TRACE   6] C: STLS\r\n
[2020-06-18 15:07:35.299320060 UTC DEBUG   6] Processing `Stls`
[2020-06-18 15:07:35.299332710 UTC DEBUG   6] 0 byte(s) remaining in buffer.
[2020-06-18 15:07:35.299422412 UTC TRACE   6] S: +OK Begin fake TLS negotiation now.\r\n
[2020-06-18 15:07:35.299442527 UTC TRACE   6] <----- Switching to TLS now ----->
[2020-06-18 15:07:35.859159766 UTC DEBUG   6] Waiting for data (`Size(4)`)
[2020-06-18 15:07:35.859370197 UTC DEBUG   6] Read 6 encrypted byte(s) via TLS.
[2020-06-18 15:07:35.859388132 UTC TRACE   6] C: CAPA\r\n
```

which feels correct, if I read it correctly.

Damian Poddebniak @duesee1 · 2 years ago Author

Perfect. Okay, the idea is now as follows: everything after `<----- Switching to TLS now ----->` is secure. An attacker should not be able to make some meaningful changes after the transition to TLS.

The `testcases/pop3/B_1.ron` file has 2 commented-out options: an option to ignore commands and an option to control the starttls response. If you leave both inactive, you should see a "normal" POP3 session and even two new messages in your mailbox.

The first command Evolution sends after starttls is the "capa" command. If you comment out the first step in the ron file, the server will simply ignore the command and not respond to it. Same for any command you put there. You should now see that Evolution "waits" for the response to the capa command, because the server just ignores it.

Edited by Damian Poddebniak 2 years ago

Damian Poddebniak @duesee1 · 2 years ago Author

And here comes the bug: by commenting out the second option (step 2), you can archieve that Evolution proceeds. This means that the data the server sent via plaintext (and an attacker can inject) is interpreted in the TLS session. The config file is configured to mimic multiple commands, but you can change it as you will. You can even mimic a whole new mailbox when providing enough answers. You can also uncomment the "ignore command" option, because a real server obviously will try to answer the commands. But the attacker commands are buffered before and are evaluated first.

Edited by Damian Poddebniak 2 years ago

Milan Crha @mcrha · 2 years ago Maintainer

Aaah, I see. I begun with SMTP, which doesn't have that chatty comments as the POP3 does. I can reproduce this and I see in libcamel logs that the extra lines, at least some of them, are processed, though I do not see (yet) whether as part of the encrypted connection or whether they are read and discarded before starting the encrypted session. For example with POP I see only once `+OK`, then `LOGIN`, then another `+OK` after `+OK Begin fake TLS negotiation now.`, but the .ron file has two more `+OK`-s and one more `LOGIN`.

No conclusion yet, it'll need more investigation.

Damian Poddebniak @duesee1 · 2 years ago Author

I am not 100% sure if I did everything correctly here, so please be cautious and check if the POP3 response is valid. Could be that I missed some newline, ".", or "+OK" response...

Damian Poddebniak @duesee1 · 2 years ago Author

Ah, I think "LOGIN" should be "USER" instead. POP3 has no "LOGIN" capability. Maybe this is interpreted as a wrong command or something.

Please register or sign in to reply

Damian Poddebniak @duesee1 · 2 years ago Author

Okay, thank you very much!

Damian Poddebniak @duesee1 · 2 years ago Author

Btw, you can add

```
        if record.level() != log::Level::Trace {
            return;
        }
```

at the top of the `log` function in src/main.rs:30 and recompile. This will suppress all, but the trace messages.

Edited by Damian Poddebniak 2 years ago

Milan Crha @mcrha · 2 years ago Maintainer

Are you able to build evolution-data-server, please? If you are on any Fedora I can provide a test package for you. I've a change which fixes it, but maybe it'll need more testing than just me.

By the way, once committed, I'll make this bug public. Feel free to remove anything private from the above comments before I'll do that.

Damian Poddebniak @duesee1 · 2 years ago Author

I can give it a try tomorrow. Can I just compile evolution-data-server with your patch and start it somehow so that my local evolution communicates with it? I use gnome and already have evolution-data-server installed. On the test server we use NixOS, not sure how to do it there.

I would also be happy if you can explain how you fixed it and why you did it that way. We found similar vulnerabilities in other software and I try to better understand the issue and the different solutions to it.

Edited by Damian Poddebniak 2 years ago

Milan Crha @mcrha · 2 years ago Maintainer

Here is the eds patch. It can be just applied and built, into the same prefix as the system eds, which will replace it. Then run Evolution and that's it.

There is no magic behind the change, it goes by road (1) from the above description. It simply truncates what had been cached in internal buffers before the STARTTLS had been confirmed. The IMAP and NNTP do not suffer of it, because they replace whole stream/cache objects, while the POP3 and SMTP left the caches filled.

It did work fine here, thus if you'd have trouble to compile then I can just commit it. You can eventually install Fedora into a virtual machine, for which I can provide test packages easily. The release is planed on July 3rd, thus we've some time for testing.

Damian Poddebniak @duesee1 · 2 years ago Author

Hm, I guess if it works for you, i.e. you are not able to inject responses anymore, it should be fine. So I guess I would prefer to spare the time in setting up eds and retesting myself. What is more important is that your patch does not introduce errors in benign connections, but you can test this a lot better than I can, for sure.

Anyway, if there is something in particular you want to test or discuss with me, I can still help out with it!

Thanks for the information you make the issue public. I "deleted" the zip.

Damian Poddebniak @duesee1 · 2 years ago Author

One more thing: I would like to have this documented in the CVE database. Shall I register a CVE or do you want to do this?

Milan Crha @mcrha · 2 years ago Maintainer

> Hm, I guess if it works for you, i.e. you are not able to inject responses anymore, it should be fine. So I guess I would prefer to spare the time in setting up eds and retesting myself.

Okay, no problem, I'll commit it.

> Shall I register a CVE or do you want to do this?

You can do that, if you want. I'll wait with the commit for some time, but not longer than before the release (which will happen on July 3rd), to have the CVE number in the commit message (for easier searching, reference, and so on).

Damian Poddebniak @duesee1 · 2 years ago Author

I registered CVE-2020-14928

Damian Poddebniak @duesee1 · 2 years ago Author

You can make the commit whenever you like and also make this issue public.

Andre Klapper changed title from **Response Injection via STARTTLS in SMTP and POP3** to **Response Injection via STARTTLS in SMTP and POP3 (CVE-2020-14928)** 2 years ago

Milan Crha @mcrha · 2 years ago Maintainer

Thanks, I'll do that.

Milan Crha changed title from **Response Injection via STARTTLS in SMTP and POP3 (CVE-2020-14928)** to **CVE-2020-14928: Response Injection via STARTTLS in SMTP and POP3** 2 years ago

Milan Crha closed via commit ba82be72 2 years ago

Milan Crha mentioned in commit f404f33f 2 years ago

Milan Crha @mcrha · 2 years ago Maintainer

The above commits are for 3.37.3+ and 3.36.4+.

Milan Crha made the issue visible to everyone 2 years ago

Michael Catanzaro @mcatanzaro · 2 years ago Developer

This broke the e-d-s build in gnome-build-meta:

```
        [945/979] Generating camel-1.2.vapi
        FAILED: src/vala/camel-1.2.vapi
        cd /buildstream/gnome/core-deps/evolution-data-server.bst/_builddir/src/vala && /usr/bin/vapigen --vapidir=/buil
        Camel-1.2.gir:53130.7-53132.22: error: overriding method `Camel.StreamBuffer.truncate' is incompatible with base
        Generation failed: 1 error(s), 0 warning(s)
```

I guess we need to decide whether overriding g_seekable_truncate() is desirable. If so, does it need to chain up to the base class truncate? Otherwise, probably should rename the function to something else?

Milan Crha @mcrha · 2 years ago Maintainer

Err, I'll rename it to `discard_cache` . (I do not build with introspection enabled usually (I prefer quicker builds), which explains why I didn't notice it.)

Milan Crha @mcrha · 2 years ago Maintainer

Also noticed that vala doesn't know what to do with `xmlNodePtr` , it only knows `xmlNode *` , which is a shame...

```
EDataServer-1.2.gir:32739.63-32739.63: error: The type name `Xml.NodePtr' could not be found
          <type name="libxml2.NodePtr" c:type="xmlNodePtr"/>
                                                              ^
make[2]: *** [src/vala/CMakeFiles/vala-files.dir/build.make:106: src/vala/libedataserver-1.2.vapi] Error 1
```

I'm going to commit both things, separately.

Milan Crha mentioned in commit 56d6ccfe 2 years ago

Milan Crha mentioned in commit b74b7651 2 years ago

Milan Crha @mcrha · 2 years ago Maintainer

The above commits are also for 3.37.3+ and 3.36.4+.

The one for the `xmlNodePtr` is 42725037 .

Please register or sign in to reply