New issue

Jump to bottom

Buffering issues with STARTTLS in IMAP #386

Closed **duesee** opened this issue on Jun 18, 2020 · 5 comments

duesee commented on Jun 18, 2020 • edited Contributor

We found a STARTTLS issue in libEtPan which affects IMAP (and probably other protocols.)

When the server responds with its "let's do TLS now message", e.g. `A OK begin TLS\r\n`, libEtPan 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 entire mailboxes even though STARTTLS is used.

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: A STARTTLS
S: A OK begin TLS
   B OK answer future login command // injected response
<--- TLS --->
C: B login user pass
// here, libEtPan interprets the injected "B OK" response and proceeds...
C: C noop
...
```

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

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.

The (maybe silly or even wrong) commit in duesee@ `5462750` #diff-b01e5693616d9ee0714273a3491bc713 seems to fix the issue (please ignore the .idea folder :P)

👍 1

Murgeye commented on Jul 23, 2020 Contributor

Hey,

have you found time to take a look at this? This might cause serious security issues in applications using libetpan to handle IMAP STARTTLS connections, as an attacker can insert plaintext into the encrypted session.

dinhvh commented on Jul 23, 2020 Owner

@duesee Could you send a pull request with your change?

duesee commented on Jul 23, 2020 Contributor Author

I opened #387

Murgeye commented on Jul 24, 2020 Contributor

The same bug is present in SMTP:

```
S: 250-example.org
S: 250 STARTTLS
C: STARTTLS
S: 220 Ready to start TLS // Injected Responses to SMTP commands follow
    250-localhost
    250 AUTH PLAIN
    250 OK
    250 OK
    250 OK
    354 End data with<CR><LF>.<CR><LF>
    250 Ok: queued
    221 BYE
<----- TLS ----->
C: EHLO Alice
C: AUTH PLAIN YXNkZgBhc2RmAGFzZGY=
C: MAIL FROM:<ALICE>
C: RCPT TO:<BOB>
C: DATA
C: Test Mail
.
C: QUIT // Libetpan does notwait for responses from the server
```

And in POP3:

```
S: +OK POP3 B1 server ready.
C: STLS
S: +OK Begin fake TLS negotiation now. // Rejected POP3 responses follow
   +OK
   +OK
   +OK
```

```
1 AAAAA
.
<----- TLS ----->
C: USER asdf
C: PASS asdf
C: LIST // libetpan does not wait for responses in encrypted context
```

I will try to send you a pull request for these as well shortly.

Murgeye mentioned this issue on Jul 24, 2020

Detect extra data after STARTTLS responses in SMTP and POP3 and exit #388

Merged

carnil commented on Jul 27, 2020

CVE-2020-15953 appears to have been assigned for this issue.

duesee closed this as completed on Jul 31, 2020

cobratbq mentioned this issue on Sep 25, 2021

Upgrade libetpan to fix CVE without introducing crashes flathub/org.claws_mail.Claws-Mail#22

Closed

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants