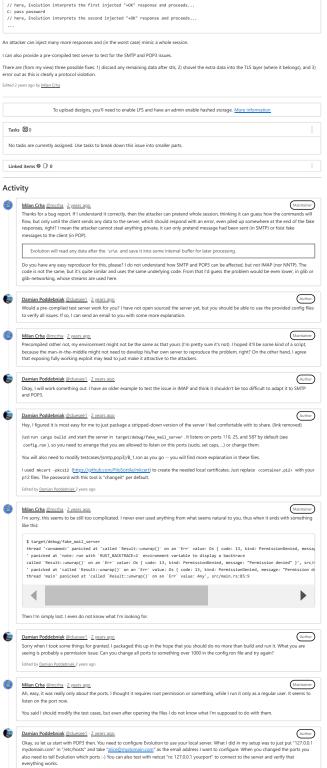
CVE-2020-14928: Response Injection via STARTTLS in SMTP and POP3

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.

Example trace to give an intuition:

L: user alice
// here, Evolution interprets the first injected "+0K" response and proceeds...
C: pass password
// here, Evolution interprets the second injected "+0K" response and proceeds...



Edited by Damian Poddebniak 2 years ago

Edited by Damian Poddel

Damian Poddebniak @dueseel - 2 years ago
If everything works, you should see a colorful trace in the terminal windows where the server is running and see what Evolution is doing,
you installed a local certificate? Since we are testing TLS, we need to provide a certificate. The easiest solution is to use the mixent tool I
mentioned eaflier. Then, just replace *container*, pt2> in the ron files in the testcases folder with the path to your pkxs12 file.

