7

CVE-2021-22947: STARTTLS protocol injection via MITM

Share:

TIMELINE

monnerat submitted a report to curl. Sep 9th (about 1 year ago)

Summary:

A man-in-the-middle can inject cleartext forged responses to future encrypted commands by pipelining them to the STARTTLS response.

Steps To Reproduce:

Use the attached test case within the curl test system. It is based on IMAP FETCH with explicit TLS. Upon test failure, the downloaded file contains "You've been hacked!" rather than the requested mail.

Impact

Mailbox content forgery (IMAP, POP3).
Sent mail content forgery (SMTP).

2 attachments:
F1442574: test981
F1442575: starttls-pipelining.patch

bagder curl staff posted a comment. Sep 9th (about 1 year ago)

Thanks. To me this looks like a clear security issue as mentioned on the mailing list previously. A mitm server can feed protocol data to curl that it will use and trust after the TLS handshake that presumably should make curl certain that it speaks to an authenticated server.

monnerat posted a comment. Sep 9th (about 1 year ago)

> Sent mail content forgery (SMTP).

My bad: not possible as it's the wrong way !

dfandrich curl staff posted a comment. Sep 9th (about 1 year ago)

At first glance I assumed that since the commands wouldn't be executed until after the TLS handshake (and therefore confirmation that we're talking to the right server) it would be unexploitable, but the light bulb went on when I realized a MITM could feed back arbitrary malicious responses before relaying the genuine TLS stream as-is. So, it sounds like a legit problem to me. There could still be SMTP shenanigans going on, even if not mail forgery (e.g., DoS on mail sending).

bagder curl staff changed the status to ○ **Triaged**. Sep 9th (about 1 year ago)

Then we confirm this as a security issue! I'll get an advisory draft going.

bagder curl staff posted a comment. Sep 9th (about 1 year ago)

This seems like an appropriate CWE: CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data

bagder curl staff updated CVE reference to CVE-2021-22947. Sep 9th (about 1 year ago)

bagder curl staff changed the report title from **Starttls response pipelining** to **CVE-2021-22947: STARTTLS email injection via MITM**. Sep 9th (about 1 year ago)

monnerat posted a comment. Sep 9th (about 1 year ago)

> There could still be SMTP shenanigans going on

So does it with FTP.

bagder curl staff posted a comment. Sep 9th (about 1 year ago)

But with FTP a mitm attacker can't trick curl into believing it is actually remote content, can it?

monnerat posted a comment. Updated Sep 9th (about 1 year ago)

No, you're right, it can't. But as with any other pingpong protocols, we could lead to a DoS, like i.e. refusing to login.

bagder curl staff posted a comment. Sep 9th (about 1 year ago)

Since the same method works across all these pingpong protocols I'll update the title and work on phrasing it better. Advisory coming up soon.

bagder curl staff changed the report title from **CVE-2021-22947: STARTTLS email injection via MITM** to **CVE-2021-22947: STARTTLS protocol injection via MITM**. Sep 9th (about 1 year ago)

bagder curl staff posted a comment. Sep 9th (about 1 year ago)

> like i.e. refusing to login.

Right, but any mitm attacker can do that (refuse to login) and we can't do anything about it...

bagder curl staff posted a comment. Sep 9th (about 1 year ago)

Here's my first advisory draft (also attached). I'm done for tonight.

STARTTLS protocol injection via MITM

VULNERABILITY

When curl connects to an IMAP, POP3, SMTP or FTP server to exchange data securely using STARTTLS to upgrade the connection to TLS level, the server can still respond and send back multiple responses before the TLS upgrade. Such multiple "pipelined" responses are cached by curl. curl would then upgrade to TLS but not flush the in-queue of cached responses and instead use and trust the responses it got *before* the TLS handshake as if they were authenticated.

Using this flaw, it allows a Man-In-The-Middle attacker to first inject the fake responses, then pass-through the TLS traffic from the legitimate server and trick curl into sending data back to the user thinking the attacker's injected data comes from the TLS-protected server.

Over POP3 and IMAP an attacker can inject fake response data.

We are not aware of any case of this flaw having been exploited in the wild.

INFO

This flaw was first introduced in commit ec3bb8f727405.

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2021-22947 to this issue.

CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data

Severity: Medium

AFFECTED VERSIONS

- Affected versions: curl 7.20.0 to and including 7.78.0
- Not affected versions: curl < 7.20.0 and curl >= 7.79.0

Also note that libcurl is used by many applications, and not always advertised as such.

THE SOLUTION

A fix for CVE-2021-22947

(The patch is gzipped to better preserve the mixed line-endings in the included three new test cases.)

RECOMMENDATIONS

A - Upgrade curl to version 7.79.0

B - Apply the patch to your local version

C - Do not use IMAP or POP3 with explicit TLS

TIMELINE

This issue was reported to the curl project on September 7, 2021.

This advisory was posted on September 15, 2021.

CREDITS

This issue was reported and patched by Patrick Monnerat.

Thanks a lot!

1 attachment:
F1443125: CVE-2021-22947.md

dfandrich curl staff posted a comment. Sep 9th (about 1 year ago)

For ftp, why couldn't the MITM server serve an EPSV response pointing to a server under its control? IIRC, curl ignores the IP address portion by default, but if an application has enabled that, it could lead to downloading data under an attacker's control.

monnerat posted a comment. Sep 9th (about 1 year ago)

A mitm can always DoS by blocking all traffic! But once TLS is negotiated, it can't react to client commands.
Our problem may direct curl (and its user) into "thinking" login credentials are not valid while they are.

monnerat posted a comment. Sep 9th (about 1 year ago)

> For ftp, why couldn't the MITM server serve an EPSV response pointing to a server under its control? IIRC, curl ignores the IP address portion by default, but if an application has enabled that, it could lead to downloading data under an attacker's control.

Yes: thus FTP data can also be affected under some conditions.

I think we can find several other such examples. This is a Pandora box!

monnerat posted a comment. Sep 9th (about 1 year ago)

> (The patch is gzipped to better preserve the mixed line-endings in the included three new test cases.)

> There are four of them?

Oops, too much copy and paste from the previous one!

bagder curl staff posted a comment. Sep 13th (about 1 year ago)

The curl security team has decided to reward hacker @monnerat with the amount of 1,500 USD for finding and reporting this issue. Many thanks for your great work!

(I'm still trying to get hackerone to invoice opencollective properly to get the funds in place for this, but it hasn't happened yet but it **will** happen eventually, sorry for the delay.)

monnerat posted a comment. Sep 13th (about 1 year ago)

Many thanks. And don't worry for the delay.

curl rewarded monnerat with a **$1,500** bounty. Sep 23rd (about 1 year ago)

bagder curl staff closed the report and changed the status to ○ **Resolved**. Sep 23rd (about 1 year ago)

bagder curl staff requested to disclose this report. Sep 23rd (about 1 year ago)

bagder curl staff disclosed this report. Sep 24th (about 1 year ago)