

8

CVE-2021-22946: Protocol downgrade required TLS bypassed

Share:     

TIMELINE



monnerat submitted a report to curl.

Sep 8th (about 1 y)

Summary:

In imap and pop3, --ssl-reqd is silently ignored if the capability command failed.

In ftp, a non-standard 230 response (preauthentication?) in the greeter message forces curl to continue unencrypted, even if TLS has been required.

Steps To Reproduce:

Use a parameterizable test server to fail capability command for imap (CAPABILITY reply: A001 BAD Not implemented) and pop3 (CAPA reply: -ERR Not implemented) and to send response code 230 in FTP server greeting message.

1. curl --ssl-reqd imap://server/...
2. curl --ssl-reqd pop3://server/...
3. curl --ssl-reqd --ftp-ssl-control ftp://server/...

These 3 commands are successful, but network sniffing shows that TLS is never negotiated.

Impact

A MitM can silently deny mandatory TLS negotiation and thus sniff and/or update unencrypted transferred data.

3 attachments:

F1441786: test985

F1441787: test986

F1441788: test984



bagder  changed the status to  Triaged.

Sep 9th (about 1 y)

Confirmed.



bagder  posted a comment.

Sep 9th (about 1 y)

@monnerat can you also attach your proposed patch here?

I'll get an advisory draft done asap as well. If we just act swiftly, this should be possible to get fixed already in 7.79.0 that's due to ship on Sep 15th.



bagder  posted a comment.

Sep 9th (about 1 y)

I believe maybe this flaw was always present in the code for IMAP and POP3, since commit <https://github.com/curl/curl/commit/ec3bb8f7274056> (Dec 12, 2009)

For FTP, I believe this commit might've introduced the issue: <https://github.com/curl/curl/commit/c5ba0c2f544653> (Apr 12, 2013)



bagder  posted a comment.

Sep 9th (about 1 y)

I'm going with [CWE-319: Cleartext Transmission of Sensitive Information](#)

Alternatively this could be [CWE-325: Missing Cryptographic Step](#)

Opinions?



bagder  posted a comment.

Sep 9th (about 1 y)

Here's my initial take at an advisory. (Also attached if you want to make a diff or something)

Protocol downgrade required TLS bypassed

Project curl Security Advisory, September 15th 2021 -

[Permalink](#)

VULNERABILITY

A user can tell curl to **require** a successful upgrade to TLS when speaking to an IMAP, POP3 or FTP server (`--ssl-reqd` on the command line or `CURLOPT_USE_SSL` set to `CURLOUSESSL_CONTROL` or `CURLOUSESSL_ALL` with libcurl). This requirement could be bypassed if the server would return a properly crafted but perfectly legitimate response.

This flaw would then make curl continue its operations **without TLS** contrary to the instructions and expectations, exposing possibly sensitive data in clear text over the network.

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](#) for IMAP

and POP3 and in

[c5ba0c2f544653](#) for FTP.

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

CWE-319: Cleartext Transmission of Sensitive Information

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-TTTT

RECOMMENDATIONS

A - Upgrade curl to version 7.79.0

B - Apply the patch to your local version

C - Do not use IMAP, POP3 or FTP

TIMELINE

This issue was reported to the curl project on September 8, 2021.

This advisory was posted on September 15, 2021.

CREDITS

This issue was reported and patched by Patrick Monnerat.

Thanks a lot!

1 attachment:
F1442129: CVE-2021-TTTT.md

 dgustafsson  posted a comment. Sep 9th (about 1 y)

I'm leaning towards [CWE-325](#) for this, while both can apply it seems to require a little less squinting. Do you have any thoughts on why 319 is more appropriate?

In the sentence below I think we should make it clear that it will downgrade without notifying the user in any way:

| .. *continue its operations without TLS contrary to the instructions* ..

Perhaps something as simple as adding "silently" could do it? : *..silently continue its operations without TLS contrary..*

 bagder  posted a comment. Sep 9th (about 1 y)

Do you have any thoughts on why 319 is more appropriate?



I couldn't really make up my mind but I had to pick one! :-) I'm totally fine with 325 too.

| Perhaps something as simple as adding "silently" could do it

Good suggestion!

I've amended my local version accordingly now.



 bagder  updated CVE reference to [CVE-2021-22946](#). Sep 9th (about 1 y)

 bagder  changed the report title from Protocol downgrading: required TLS ignored to CVE-2021-22946: Protocol downgrade required TLS bypassed. Sep 9th (about 1 y)



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

Here is the patch

1 attachment:
F1442222: 0001-ftp-imap-pop3-do-not-ignore-ssl-reqd.patch

 bagder  posted a comment. Sep 9th (about 1 y)

If anyone tries to apply that patch and tries the new tests (bonus points for those @monnerat !): patch tends to lose the mixed CRLF line endings in the test cases they might need a minor manual edit to work correctly.

 bagder  added weakness "Missing Required Cryptographic Step" and removed weakness "Man-in-the-Middle". Sep 9th (about 1 y)

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

The patch without the tests

1 attachment:
F1442256: cve-2021-22946.patch

(I'm still trying to get hackone10 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 y

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



curl rewarded monnerat with a \$1,000 bounty.

Sep 23rd (about 1 y



bagder curl staff closed the report and changed the status to **Resolved**.

Sep 23rd (about 1 y



bagder curl staff requested to disclose this report.

Sep 23rd (about 1 y



bagder curl staff disclosed this report.

Sep 24th (about 1 y