# CVE-2021-22946: Protocol downgrade required TLS bypassed



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.

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

Use a parameterizable test server to fail capability command for imap (CAPABILITY reply: A001 BAD Not implemented) and pop3 (CAPA reply: -ERR Not implement 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 successsful, but network sniffing shows that TLS is never negotiated.

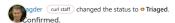
A MitM can silently deny mandatory TLS negotiation and thus sniff and/or update unencrypted transferred data.

3 attachments:

F1441786: test985

F1441787: test986

F1441788: test984





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.



gder (curl staff) posted a comment.

Sep 9th (about 1 v

believe maybe this flaw was always present in the code for IMAP and POP3, since commit https://github.com/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)



gder curl staff posted a comment. agder Curl start / posted a comment.

m going with CWE-319: Cleartext Transmission of Sensitive Information Sep 9th (about 1 y

Alternatively this could be CWE-325: Missing Cryptographic Step

Opinions?



igder (curl staff) posted a comment.

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

Sep 9th (about 1 v

# 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 ( --ss1-reqd on the command line or CURLOPT\_USE\_SSL set to CURLUSESSL\_CONTROL or CURLUSESSL\_ALL with libcurl). This requirement could be by passed 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 value abilities and Exposures (CVE) project has assigned the name

CVE-2021-TTTTT 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-TTTTT

## 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-TTTTT.md

dgustafsson (curl staff) posted a comment.

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 ..

igder curl staff posted a comment. agder (curl staff) posted a comment.

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

Sep 9th (about 1 v

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.

O-bagder curl staff updated CVE reference to CVE-2021-22946.

Sep 9th (about 1 y

- bagder curl staff changed the report title from Protocol downgrading: required TLS ignored to CVE-2021-22946: Protocol downgrade required TLS bypassed.

Sep 9th (about 1 y Sep 9th (about 1 y

monnerat posted a comment. Here is the patch

1 attachment:

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

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

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

Sep 9th (about 1 y

monnerat posted a comment. The patch without the tests

Sep 9th (about 1 y

1 attachment:

F1442256: cve-2021-22946.patch

ti matin dying to get natherone to invoice open conecuve properly to get the rands in place for this, out it hash thappened yet out it will happened the delay.)	ericually, sorry i
monnerat posted a comment.  Many thanks. And don't worry for the delay.	Sep 13th (about 1 y
O- curl rewarded monnerat with a \$1,000 bounty.	Sep 23rd (about 1 y
O-bagder curt staff closed the report and changed the status to O Resolved.	Sep 23rd (about 1 y
O-bagder curl staff requested to disclose this report.	Sep 23rd (about 1 y
O=bagder	Sep 24th (about 1 y