10 **CVE-2021-22897: schannel cipher selection surprise**

Share:

TIMELINE

nyymi submitted a report to curl. Apr 22nd (2 ye

Summary:

Commit "schannel: support selecting ciphers" added support for selecting the ciphers with SCHANNEL. However, due to use of a static `algIds` array for ciphers i `set_ssl_ciphers` the last configured cipher list will override configuration used by other connections, leading to potential wrong configuration for them. This may security implications if insecure cipher configuration is used where secure cipher configuration is expected.

Steps To Reproduce:

1.Create two or more separate curl handles with `curl_easy_init`
2. Set different cipher lists with `curl_easy_setopt` `CURLOPT_SSL_CIPHER_LIST` to the curl handles
3. Create simultaneous connections with there the separate curl handles

Instead of each connection using the specific cipher list some of them will share the wrong configuration. If/how this happens exactly depends on how the connec setup overlaps.

Note that to be vulnerable some existing application using libcurl would needs to use such mixed `CURLOPT_SSL_CIPHER_LIST` configuration with multiple curl handle begin with. It is not really known how likely this really is, but it seems somewhat rare use case.

Supporting Material/References:

- Commit adding the vulnerable feature: https://github.com/curl/curl/commit/9aefbff30d280c60fc9d8cc3e0b2f19fc70a2f28

Impact

Potentially wrong cipher configuration used for connections.

bagder curl staff posted a comment. Updated Apr 22nd (2 ye
Thanks, we'll check it out!

bagder curl staff posted a comment. Apr 22nd (2 ye
BTW, Since this is code not yet in a release, we don't consider it an actual security problem.

nyymi posted a comment. Apr 22nd (2 ye
It is somewhat difficult to calculate the "correct" CVSS score for this vulnerability, so the value currently calculated might be off. The actual impact wildly depends external factors, such as for example whether it is even possible to select insecure cipher configurations with SChannel to begin with. I can imagine situations whe some application would for example allow user to configure cipher selection for *some* connections, while it should not affect cipher selection for other, more secu connections. In such setup this confusion might actually be impactful.

nyymi posted a comment. Apr 22nd (2 ye
Hmm, I see the code in question in the 7.76.1 release at least.

```
static ALG_ID algIds[45]; /*There are 45 listed in the MS headers*/
```

Is it just dead code?

bagder curl staff posted a comment. Apr 23rd (2 ye
Ah, sorry I might be confusing commits. I'll verity that as well.

bagder curl staff updated the severity from None to Low. Apr 23rd (2 ye

bagder curl staff changed the status to ○ **Triaged**. Updated Apr 23rd (2 ye
This is indeed a genuine and security related problem exactly as reported and described by @nyymi . This has existed since libcurl 7.61.0 with the commit linked ab CVSS is tricky for this, but I think "Low" still seems fair. Feel free to tell me how I'm wrong on this.

I have an initial proposed patch attached, but I haven't actually test-built it on Windows so could be fatally flawed.

@nyymi: I would like to work on this fix and corresponding advisory and announce it in sync with the planned next curl release (7.77.0) on May 26. You okay with thi

1 attachment:
F1275704: 0001-schannel-don-t-use-static-to-store-selected-ciphers.patch

nyymi posted a comment. Apr 23rd (2 ye
This is fine with me.

bagder curl staff posted a comment. Apr 27th (2 ye
I think CWE-488: Exposure of Data Element to Wrong Session sounds like an accurate CWE, thoughts?

https://cwe.mitre.org/data/definitions/488.html

bagder curl staff updated CVE reference to CVE-2021-22897. Apr 27th (2 ye agder curl staff posted a comment. Apr 27th (2 ye

irst take on advisory (also attached)

schannel cipher selection surprise

Project curl Security Advisory, May 26th 2021 -
Permalink

VULNERABILITY

libcurl lets applictions specify which specific TLS ciphers to use in transfers, using the option called `CURLOPT_SSL_CIPHER_LIST`. The cipher selection is used for the TLS negotation when a transfer is done involving any of the TLS based transfer protocols libcurl supports, such as HTTPS, FTPS, IMAPS, POP3S, SMTPS etc.

Due to a mistake in the code, the selected cipher set was stored in a single "static" variable in the library, which has the surprising side-effect that if an application sets up multiple concurrent transfers, the last one that sets the ciphers will accidentally control the set used by all transfers. In a worst-case scenario, this weakens transport security significantly.

We are not aware of any exploit of this flaw.

INFO

This flaw has existed in libcurl since commit
9aefbff30d280c60fc
in libcurl 7.61.0, released on July 11, 2018.

It can only trigger when Schannel is used, which is the native TLS library in Microsoft Windows.

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2021-22897 to this issue.

CWE-488: Exposure of Data Element to Wrong Session

Severity: Low

AFFECTED VERSIONS

This issue only exists when libcurl is built to use Schannel.

- Affected versions: libcurl 7.61.0 to and including 7.76.1
- Not affected versions: libcurl < 7.61.0 and libcurl >= 7.77.0

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

THE SOLUTION

Store the cipher selection in data associated with the connection.

A fix for CVE-2021-22897

(The patch URL will change in the final published version of this advisory)

RECOMMENDATIONS

If you're using an Schannel based libcurl, We suggest you take one of the following actions immediately, in order of preference:

A - Upgrade libcurl to version 7.77.0

B - Apply the patch to your local version

C - Avoid using `CURLOPT_SSL_CIPHER_LIST`

TIMELINE

This issue was reported to the curl project on April 23, 2021.

This advisory was posted on May 26, 2021.

CREDITS

This issue was reported by Harry Sintonen. Patch by Daniel Stenberg.

Thanks a lot!

1 attachment:
F1280430: CVE-2021-22897.md

nyymi posted a comment. Apr 27th (2 ye

CWE-488 is a good match here, indeed. Advisory text is looking good as well.

rl rewarded nyymi with a **$800** bounty. May 7th (2 ye bagder curl staff requested to disclose this report. May 26th (2 ye

nyymi agreed to disclose this report. May 26th (2 ye

This report has been disclosed. May 26th (2 ye