



Products

Services

Publications

Resources

What's new

Follow @Openwall on Twitter for new release announcements and other news

[<prev] [next>] [day] [month] [year] [list]

Message-ID: <nycvar.QR0.7.76.2107210915010.25537@fvvyl>
Date: Wed, 21 Jul 2021 09:15:24 +0200 (CEST)
From: Daniel Stenberg <daniel@...x.se>
To: curl security announcements -- curl users <curl-users@...l.haxx.se>,
curl-announce@...l.haxx.se, libcurl hacking <curl-library@...l.haxx.se>,
oss-security@...ts.openwall.com
Subject: [SECURITY ADVISORY] curl: TELNET stack contents disclosure again

TELNET stack contents disclosure again

Project curl Security Advisory, July 21st 2021 -
[Permalink](<https://curl.se/docs/CVE-2021-22925.html>)

VULNERABILITY

curl supports the `-t` command line option, known as `CURLOPT_TELNETOPTIONS` in libcurl. This rarely used option is used to send variable=content pairs to TELNET servers.

Due to flaw in the option parser for sending `NEW_ENV` variables, libcurl could be made to pass on uninitialized data from a stack based buffer to the server. Therefore potentially revealing sensitive internal information to the server using a clear-text network protocol.

This could happen because curl did not call and use `sscanf()` correctly when parsing the string provided by the application.

The previous curl security vulnerability [CVE-2021-22898](<https://curl.se/docs/CVE-2021-22898.html>) is almost identical to this one but the fix was insufficient so this security vulnerability remained.

We are not aware of any exploit of this flaw.

INFO

This flaw has existed in curl since commit [ald6ad2610](<https://github.com/curl/curl/commit/ald6ad2610>) in libcurl 7.7, released on March 22, 2001. There was a previous attempt to fix this issue in curl 7.77.0 but it was not done proper.

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2021-22925 to this issue.

CWE-457: Use of Uninitialized Variable

Severity: Medium

AFFECTED VERSIONS

- Affected versions: curl 7.7 to and including 7.77.0
- Not affected versions: curl < 7.7 and curl >= 7.78.0

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

THE SOLUTION

Use `sscanf()` properly and only use properly filled-in buffers.

A [fix for CVE-2021-22925] (<https://github.com/curl/curl/commit/894f6ec730597eb243618d33cc84d71add8d6a8a>)

RECOMMENDATIONS

- A - Upgrade curl to version 7.78.0
- B - Apply the patch to your local version
- C - Avoid using `CURLOPT_TELNETOPTIONS`

TIMELINE

This issue was reported to the curl project on June 11, 2021.

This advisory was posted on July 21, 2021.

CREDITS

This issue was reported and patched by Red Hat Product Security.

Thanks a lot!

--

```
/ daniel.haxx.se  
| Commercial curl support up to 24x7 is available!  
| Private help, bug fixes, support, ports, new features  
| https://www.wolfssl.com/contact/
```

Powered by [blists](#) - [more mailing lists](#)

Please check out the [Open Source Software Security Wiki](#), which is counterpart to this [mailing list](#).

Confused about [mailing lists](#) and their use? [Read about mailing lists on Wikipedia](#) and check out these [guidelines on proper formatting of your messages](#).