CVE-2021-22898

Awarded 1000 USD

Related:
Audits
Changelog
curl CVEs
JSON metadata
Original report
Vulnerability Disclosure
Vulnerabilities Table

TELNET stack contents disclosure

Project curl Security Advisory, May 26 2021
Permalink

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 check the return code from a `sscanf(command, "%127[^,],%127s")` function invoke correctly, and would leave the piece of the send buffer uninitialized for the value part if it was provided longer than 127 bytes. The buffer used for this is 2048 bytes big and the *variable* part of the *variable=content* pairs would be stored correctly in the send buffer, making curl sending "interleaved" bytes sequences of stack contents. A single curl TELNET handshake could then be made to send off a total of around 1800 bytes of (non-contiguous) stack contents in this style:

```
[control byte]name[control byte]
stack contents
[control byte]name[control byte]
stack contents
...
```

An easy proof of concept command line looks like this:

```
curl telnet://example.com -tNEW_ENV=a,bbbbbb (256 'b's)
```

INFO

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2021-22898 to this issue.

CWE-457: Use of Uninitialized Variable

Severity: Medium

AFFECTED VERSIONS

- Affected versions: curl 7.7 to and including 7.76.1
- Not affected versions: curl < 7.7 and curl >= 7.77.0
- Introduced-in: https://github.com/curl/curl/commit/a1d6ad2610

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

SOLUTION

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

- Fixed-in: https://github.com/curl/curl/commit/39ce47f219b09c380b81f89fe

RECOMMENDATIONS

A - Upgrade curl to version 7.77.0

B - Apply the patch to your local version

C - Avoid using `CURLOPT_TELNETOPTIONS`

TIMELINE

This issue was reported to the curl project on April 27, 2021.

This advisory was posted on May 26, 2021.

CREDITS

- Reported-by: Harry Sintonen
- Patched-by: Harry Sintonen

Thanks a lot!