CVE-2017-1000100

TFTP sends more than buffer size

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

Project curl Security Advisory, August 9 2017
Permalink

VULNERABILITY

When doing a TFTP transfer and curl/libcurl is given a URL that contains a long filename (longer than about 515 bytes), the filename is truncated to fit within the buffer boundaries, but the buffer size is still wrongly updated to use the original length. This too large value is then used in the `sendto()` call, making curl attempt to send more data than what is actually put into the buffer. The `sendto()` function then reads beyond the end of the heap based buffer.

A malicious HTTP(S) server could redirect a vulnerable libcurl-using client to a crafted TFTP URL (if the client has not restricted which protocols it allows redirects to) and trick it to send private memory contents to a remote server over UDP. Limit curl's redirect protocols with `--proto-redir` and libcurl's with `CURLOPT_REDIR_PROTOCOLS`.

INFO

This flaw also affects the curl command line tool.

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2017-1000100 to this issue.

CWE-126: Buffer Over-read

Severity: High

AFFECTED VERSIONS

- Affected versions: libcurl 7.15.0 to and including 7.54.1
- Not affected versions: libcurl < 7.15.0 and >= 7.55.0
- Introduced-in: https://github.com/curl/curl/commit/56d9624b566

libcurl is used by many applications, but not always advertised as such.

SOLUTION

The function now returns error if attempting to send a filename that is too long to fit in the TFTP packet.

- Fixed-in: https://github.com/curl/curl/commit/358b2b131ad6c095696f20dc

RECOMMENDATIONS

We suggest you take one of the following actions immediately, in order of preference:

A - Upgrade curl and libcurl to version 7.55.0

B - Apply the patch to your version and rebuild

C - Disable TFTP or otherwise restrict TFTP transfers

TIMELINE

It was reported to the curl project on July 11, 2017. We contacted distros@openwall on August 1.

libcurl 7.55.0 was released on August 9 2017, coordinated with the publication of this advisory.

CREDITS

- Reported-by: Even Rouault
- Patched-by: Daniel Stenberg

Discovery: credit to OSS-Fuzz.

Thanks a lot!