CVE-2017-8816

NTLM buffer overflow via integer overflow

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

Project curl Security Advisory, November 29 2017
Permalink

VULNERABILITY

libcurl contains a buffer overrun flaw in the NTLM authentication code.

The internal function `Curl_ntlm_core_mk_ntlmv2_hash` sums up the lengths of the username + password (= SUM) and multiplies the sum by two (= SIZE) to figure out how large storage to allocate from the heap.

The SUM value is subsequently used to iterate over the input and generate output into the storage buffer. On systems with a 32-bit `size_t`, the math to calculate SIZE triggers an integer overflow when the combined lengths of the username and password is larger than 2GB (2^31 bytes). This integer overflow usually causes a tiny buffer to actually get allocated instead of the intended huge one, making the use of that buffer end up in a buffer overrun.

INFO

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2017-8816 to this issue.

CWE-131: Incorrect Calculation of Buffer Size

Severity: Medium

AFFECTED VERSIONS

This is only an issue on 32-bit systems. It also requires the user and password fields to use more than 2GB of memory combined, which in itself should be rare.

- Affected versions: libcurl 7.36.0 to and including 7.56.1
- Not affected versions: libcurl < 7.36.0 and >= 7.57.0
- Introduced-in: https://github.com/curl/curl/commit/86724581b6c02d160b5

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

SOLUTION

In libcurl version 7.57.0, the integer overflow is avoided.

- Fixed-in: https://github.com/curl/curl/commit/7f2a1df6f5fc598750b2c

RECOMMENDATIONS

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

A - Upgrade curl to version 7.57.0

B - Apply the patch to your version and rebuild

C - Put length restrictions on the username and passwords you can pass to libcurl

TIMELINE

It was reported to the curl project on November 6, 2017. We contacted distros@openwall on November 21.

curl 7.57.0 was released on November 29 2017, coordinated with the publication of this advisory.

CREDITS

- Reported-by: Alex Nichols
- Patched-by: Daniel Stenberg

Thanks a lot!