CVE-2018-14618

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

NTLM password overflow via integer overflow

Project curl Security Advisory, September 5th 2018 - Permalink

VULNERABILITY

libcurl contains a buffer overrun in the NTLM authentication code.

The internal function `Curl_ntlm_core_mk_nt_hash` multiplies the `length` of the password by two (SUM) to figure out how large temporary storage area to allocate from the heap.

The `length` value is then subsequently used to iterate over the password and generate output into the allocated storage buffer. On systems with a 32-bit `size_t`, the math to calculate SUM triggers an integer overflow when the password length exceeds 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 heap buffer overflow.

(This bug is almost identical to CVE-2017-8816.)

INFO

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2018-14618 to this issue.

CWE-131: Incorrect Calculation of Buffer Size

Severity: High

AFFECTED VERSIONS

This issue is only present on 32-bit systems. It also requires the password field to use more than 2GB of memory, which should be rare.

- Affected versions: libcurl 7.15.4 to and including 7.61.0
- Not affected versions: libcurl < 7.15.4 and >= 7.61.1
- Introduced-in: https://github.com/curl/curl/commit/be285cde3f

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

SOLUTION

In libcurl version 7.61.1, the integer overflow is avoided.

- Fixed-in: https://github.com/curl/curl/commit/57d299a499155d4b327e34

RECOMMENDATIONS

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

A - Upgrade curl to version 7.61.1

B - Apply the patch to your version and rebuild

C - Put length restrictions on the password you can pass to libcurl

TIMELINE

It was publicly reported to the curl project on July 18, 2018. We contacted distros@openwall on August 27.

curl 7.61.1 was released on September 5 2018, coordinated with the publication of this advisory.

CREDITS

- Reported-by: Zhaoyang Wu
- Patched-by: Daniel Stenberg

Thanks a lot!