CVE-2019-3822

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

NTLMv2 type-3 header stack buffer overflow

Project curl Security Advisory, February 6th 2019 - Permalink

VULNERABILITY

libcurl contains a stack based buffer overflow vulnerability.

The function creating an outgoing NTLM type-3 header (`lib/vauth/ntlm.c:Curl_auth_create_ntlm_type3_message()`), generates the request HTTP header contents based on previously received data. The check that exists to prevent the local buffer from getting overflowed is implemented wrongly (using unsigned math) and as such it does not prevent the overflow from happening.

This output data can grow larger than the local buffer if large response data is extracted from a previous NTLMv2 header provided by the malicious or broken HTTP server.

Such large response data needs to be around 1000 bytes or more. The actual payload data copied to the target buffer comes from the NTLMv2 type-2 response header.

INFO

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2019-3822 to this issue.

CWE-121: Stack-based Buffer Overflow

Severity: High

AFFECTED VERSIONS

Not every libcurl build has this code enabled. For example, it is not present when building with OpenSSL with MD4 disabled. See `lib/curl_ntlm_core.h` for details.

- Affected versions: libcurl 7.36.0 to and including 7.63.0
- Not affected versions: libcurl < 7.36.0 and >= 7.64.0
- Introduced-in: https://github.com/curl/curl/commit/86724581b6c

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

SOLUTION

- Fixed-in: https://github.com/curl/curl/commit/50c9484278c63b958655a7

RECOMMENDATIONS

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

A - Upgrade curl to version 7.64.0

B - Apply the patch to your version and rebuild

C - Turn off NTLM authentication

TIMELINE

It was reported to the curl project on December 30, 2018. We contacted distros@openwall on January 28.

curl 7.64.0 was released on February 6 2019, coordinated with the publication of this advisory.

CREDITS

- Reported-by: Wenxiang Qian of Tencent Blade Team
- Patched-by: Daniel Stenberg
- Help-by: Huzaifa Sidhpurwala

Thanks a lot!