CVE-2018-16890

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

NTLM type-2 out-of-bounds buffer read

Project curl Security Advisory, February 6 2019
Permalink

VULNERABILITY

libcurl contains a heap buffer out-of-bounds read flaw.

The function handling incoming NTLM type-2 messages (`lib/vauth/ntlm.c:ntlm_decode_type2_target`) does not validate incoming data correctly and is subject to an integer overflow vulnerability.

Using that overflow, a malicious or broken NTLM server could trick libcurl to accept a bad length + offset combination that would lead to a buffer read out-of-bounds.

INFO

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2018-16890 to this issue.

CWE-125: Out-of-bounds Read

Severity: Medium

AFFECTED VERSIONS

- 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/b780b30d1377adb10bbe77

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

Thanks a lot!