CVE-2018-16840

Awarded 100 USD

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

use after free in handle close

Project curl Security Advisory, October 31st 2018 - Permalink

VULNERABILITY

libcurl contains a heap use after free flaw in code related to closing an easy handle.

When closing and cleaning up an "easy" handle in the `Curl_close()` function, the library code first frees a struct (without clearing the pointer) and might then subsequently erroneously write to a struct field within that already freed struct.

INFO

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2018-16840 to this issue.

CWE-416: Use After Free

Severity: Low

AFFECTED VERSIONS

- Affected versions: libcurl 7.59.0 to and including 7.61.1
- Not affected versions: libcurl < 7.59.0 and >= 7.62.0
- Introduced-in: https://github.com/curl/curl/commit/b46cfbc068

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

SOLUTION

- Fixed-in: https://github.com/curl/curl/commit/81d135d67155c5295b10336

RECOMMENDATIONS

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

A - Upgrade curl to version 7.62.0

B - Apply the patch to your version and rebuild

TIMELINE

It was reported to the curl project on October 14, 2018. We contacted distros@openwall on October 22.

curl 7.62.0 was released on October 31 2018, coordinated with the publication of this advisory.

CREDITS

- Reported-by: Brian Carpenter (Geeknik Labs)
- Patched-by: Daniel Stenberg

Thanks a lot!