CVE-2016-8622

URL unescape heap overflow via integer truncation

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

Project curl Security Advisory, November 2 2016 Permalink

VULNERABILITY

The URL percent-encoding decode function in libcurl is called `curl_easy_unescape`. Internally, even if this function would be made to allocate a destination buffer larger than 2GB, it would return that new length in a signed 32-bit integer variable, thus the length would get either just truncated or both truncated and turned negative. That could then lead to libcurl writing outside of its heap based buffer.

This can be triggered by a user on a 64-bit system if the user can send in a custom (large) URL to a libcurl using program.

INFO

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2016-8622 to this issue.

CWE-122: Heap-based Buffer Overflow

Severity: Medium

AFFECTED VERSIONS

This flaw exists in the following curl versions

- Affected versions: curl 7.24.0 to and including 7.50.3
- Not affected versions: curl < 7.24.0 and curl >= 7.51.0
- Introduced-in: https://github.com/curl/curl/commit/75ca568fa1

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

SOLUTION

In version 7.51.0, the parser function is fixed.

- Fixed-in: https://github.com/curl/curl/commit/53e71e47d6b81650d26ec33a5

RECOMMENDATIONS

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

A - Upgrade curl and libcurl to version 7.51.0

B - Apply the patch to your version and rebuild

TIMELINE

It was first reported to the curl project on September 23 by Cure53.

We contacted distros@openwall on October 19.

curl 7.51.0 was released on November 2 2016, coordinated with the publication of this advisory.

CREDITS

- Reported-by: Cure53
- Patched-by: Daniel Stenberg

his vulnerability was found during a Secure Open Source audit performed by Cure53.