CVE-2016-8620

glob parser write/read out of bounds

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

Project curl Security Advisory, November 2 2016
Permalink

VULNERABILITY

The curl tool's "globbing" feature allows a user to specify a numerical range through which curl iterates. It is typically specified as `[1-5]`, specifying the first and the last numbers in the range. Or with `[a-z]`, using letters.

1. The curl code for parsing the second *unsigned* number did not check for a leading minus character, which allowed a user to specify `[1--1]` with no complaints and have the latter `-1` number get turned into the largest unsigned long value the system can handle. This would ultimately cause curl to write outside the dedicated heap allocated buffer after no less than 100,000 iterations, since it would have room for 5 digits but not 6.

2. When the range is specified with letters, and the ending letter is left out `[L-]`, the code would still advance its read pointer 5 bytes even if the string was just 4 bytes and end up reading outside the given buffer.

This flaw exists only in the curl tool, not in the libcurl library.

INFO

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2016-8620 to this issue.

CWE-122: Heap-based Buffer Overflow

Severity: Medium

AFFECTED VERSIONS

This flaw exists in the following curl versions.

- Affected versions: curl 7.34.0 to and including 7.50.3
- Not affected versions: curl < 7.34.0 and curl >= 7.51.0

SOLUTION

In version 7.51.0, the function reading data considers reading a zero size to be an error and bails out.

- Fixed-in: https://github.com/curl/curl/commit/fbb5f1aa0326d485d5a7ac643

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

C - Switch off globbing or make sure you have all ranges in use verified!

TIMELINE

It was first reported to the curl project on October 2 2016.

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: Luật Nguyễn
- Patched-by: Daniel Stenberg

Thanks a lot!