CVE-2018-1000301

RTSP bad headers buffer over-read

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

Project curl Security Advisory, May 16 2018
Permalink

VULNERABILITY

curl can be tricked into reading data beyond the end of a heap based buffer used to store downloaded content.

When servers send RTSP responses back to curl, the data starts out with a set of headers. curl parses that data to separate it into a number of headers to deal with those appropriately and to find the end of the headers that signal the start of the "body" part.

The function that splits up the response into headers is called `Curl_http_readwrite_headers()` and in situations where it cannot find a single header in the buffer, it might end up leaving a pointer pointing into the buffer instead of to the start of the buffer which then later on may lead to an out of buffer read when code assumes that pointer points to a full buffer size worth of memory to use.

This could potentially lead to information leakage but most likely a crash/denial of service for applications if a server triggers this flaw.

INFO

This bug was originally introduced in May 2003 in this commit but it did not become a problem until we added RTSP in January 2010 in this commit.

We have only proven this to trigger with RTSP traffic even though this is code shared with HTTP. We believe this is not a problem for HTTP transfers.

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2018-1000301 to this issue.

CWE-126: Buffer Over-read

Severity: Medium

AFFECTED VERSIONS

- Affected versions: curl 7.20.0 to and including curl 7.59.0
- Not affected versions: curl < 7.20.0 and curl >= 7.60.0
- Introduced-in: https://github.com/curl/curl/commit/bc4582b68a673d3

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

SOLUTION

In curl version 7.60.0, curl makes sure to restore the pointer back to where its supposed to point.

- Fixed-in: https://github.com/curl/curl/commit/8c7b3737d29ed5c0575bf5

RECOMMENDATIONS

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

A - Upgrade curl to version 7.60.0

B - Apply the patch to your version and rebuild

TIMELINE

It was reported to the curl project on March 24, 2018

We contacted distros@openwall on May 7, 2018.

curl 7.60.0 was released on May 16 2018, coordinated with the publication of this advisory.

CREDITS

- Reported-by: OSS-Fuzz
- Help-by: Max Dymond
- Patched-by: Daniel Stenberg

Thanks a lot!