CVE-2017-1000257

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

IMAP FETCH response out of bounds read

Project curl Security Advisory, October 23rd 2017 - Permalink

VULNERABILITY

libcurl contains a buffer overrun flaw in the IMAP handler.

An IMAP FETCH response line indicates the size of the returned data, in number of bytes. When that response says the data is zero bytes, libcurl would pass on that (non-existing) data with a pointer and the size (zero) to the deliver-data function.

libcurl's deliver-data function treats zero as a magic number and invokes strlen() on the data to figure out the length. The strlen() is called on a heap based buffer that might not be zero terminated so libcurl might read beyond the end of it into whatever memory lies after (or just crash) and then deliver that to the application as if it was actually downloaded.

INFO

This bug was introduced when the initial support for IMAP was introduced.

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2017-1000257 to this issue.

CWE-126: Buffer Over-read

Severity: Medium

AFFECTED VERSIONS

- Affected versions: libcurl 7.20.0 to and including 7.56.0
- Not affected versions: libcurl < 7.20.0 and >= 7.56.1
- Introduced-in: https://github.com/curl/curl/commit/ec3bb8f727

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

SOLUTION

In libcurl version 7.56.1, a zero bytes response is not passed on.

- Fixed-in: https://github.com/curl/curl/commit/13c9a9ded3ae744a1e11cbc14e9146d9fa427040

RECOMMENDATIONS

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

A - Upgrade curl to version 7.56.1

B - Apply the patch to your version and rebuild

C - Switch off IMAP in `CURLOPT_PROTOCOLS`

TIMELINE

It was reported to the curl project on October 6, 2017. We contacted distros@openwall on October 17.

curl 7.56.1 was released on October 23 2017, coordinated with the publication of this advisory.

CREDITS

- Reported-by: Brian Carpenter (Geeknik Labs), 0xd34db347
- Patched-by: Daniel Stenberg

Also independently detected by and reported by the OSS-Fuzz project.

Thanks a lot!