CVE-2016-8617

OOB write via unchecked multiplication

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

Project curl Security Advisory, November 2, 2016 - Permalink

VULNERABILITY

In libcurl's base64 encode function, the output buffer is allocated as follows without any checks on `insize`:

```
malloc( insize * 4 / 3 + 4 )
```

On systems with 32-bit addresses in userspace (e.g. x86, ARM, x32), the multiplication in the expression wraps around if `insize` is at least 1GB of data. If this happens, an undersized output buffer is allocated, but the full result is written, thus causing the memory behind the output buffer to be overwritten.

If a username is set directly via `CURLOPT_USERNAME` (or curl's `-u, --user` option), this vulnerability can be triggered. The name has to be at least 512MB big in a 32-bit system.

Systems with 64-bit versions of the `size_t` type are not affected by this issue.

INFO

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2016-8617 to this issue.

CWE-131: Incorrect Calculation of Buffer Size

Severity: Medium

AFFECTED VERSIONS

This flaw exists in the following curl versions.

- Affected versions: curl 7.8.1 to and including 7.50.3
- Not affected versions: curl < 7.8.1 and curl >= 7.51.0
- Introduced-in: https://github.com/curl/curl/commit/00b00c693127d9e3a4ee

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

SOLUTION

In version 7.51.0, the overflow is avoided.

- Fixed-in: https://github.com/curl/curl/commit/efd24d57426bd77c9b5860e6b2

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 - Do not use the `CURLOPT_USERNAME` option.

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

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