CVE-2016-9586

printf floating point buffer overflow

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

Project curl Security Advisory, December 21, 2016 - Permalink

VULNERABILITY

libcurl's implementation of the printf() functions triggers a buffer overflow when doing a large floating point output. The bug occurs when the conversion outputs more than 255 bytes.

The flaw happens because the floating point conversion is using system functions without the correct boundary checks.

The functions have been documented as deprecated for a long time and users are discouraged from using them in "new programs" as they are planned to get removed at a future point. Since the functions are present and there is nothing preventing users from using them, we expect there to be a certain amount of existing users in the wild.

If there are any application that accepts a format string from the outside without necessary input filtering, it could allow remote attacks.

This flaw does not exist in the command line tool.

INFO

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2016-9586 to this issue.

CWE-121: Stack-based Buffer Overflow

Severity: Medium

AFFECTED VERSIONS

This flaw exists in the following libcurl versions.

- Affected versions: curl 5.4 to and including 7.51.0
- Not affected versions: curl < 5.4 and curl >= 7.52.0
- Introduced-in: https://github.com/curl/curl/commit/ae1912cb0d494b48d514d

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

SOLUTION

In version 7.52.0, the conversion is limited to never generate a larger output than what fits in the fixed size buffer.

- Fixed-in: https://github.com/curl/curl/commit/3ab3c16db6a5674f53cf23d565

RECOMMENDATIONS

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

A - Upgrade curl and libcurl to version 7.52.0

B - Apply the patch to your version and rebuild

C - Do not use the `curl_mprintf()` functions

TIMELINE

It was first reported to the curl project on November 8 by Daniel Stenberg.

We contacted distros@openwall on December 13.

curl 7.52.0 was released on December 21 2016, coordinated with the publication of this advisory.

CREDITS

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

Thanks a lot!