CVE-2018-16839

SASL password overflow via integer overflow

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

Project curl Security Advisory, October 31 2018 Permalink

VULNERABILITY

libcurl contains a buffer overrun in the SASL authentication code.

The internal function `Curl_auth_create_plain_message` fails to correctly verify that the passed in lengths for name and password are not too long, then calculates a buffer size to allocate.

On systems with a 32-bit `size_t`, the math to calculate the buffer size triggers an integer overflow when the username length exceeds 1GB and the password name length is close to 2GB in size. This integer overflow usually causes a tiny buffer to actually get allocated instead of the intended huge one, making the use of that buffer end up in a heap buffer overflow.

(This bug is similar to CVE-2018-14618.)

INFO

The affected function can only be invoked when using POP3(S), IMAP(S) or SMTP(S).

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2018-16839 to this issue.

CWE-131: Incorrect Calculation of Buffer Size

Severity: Low

AFFECTED VERSIONS

This issue is only present on 32-bit systems. It also requires the username field to use more than 2GB of memory, which should be rare.

- Affected versions: libcurl 7.33.0 to and including 7.61.1
- Not affected versions: libcurl < 7.33.0 and >= 7.62.0
- Introduced-in: https://github.com/curl/curl/commit/c56f9797e7feb7c2dc

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

SOLUTION

In libcurl version 7.62.0, the integer overflow is avoided. An error is returned if a too long username is attempted.

- Fixed-in: https://github.com/curl/curl/commit/f3a24d7916b9173c69a3e0ee79

RECOMMENDATIONS

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

A - Upgrade curl to version 7.62.0

B - Apply the patch to your version and rebuild

C - Put length restrictions on the username field you can pass to libcurl

TIMELINE

It was reported to the curl project on September 6, 2018. We contacted distros@openwall on October 22.

curl 7.62.0 was released on October 31 2018, coordinated with the publication of this advisory.

CREDITS

- Reported-by: Harry Sintonen
- Patched-by: Daniel Stenberg

Thanks a lot!