Security Advisory 2023-076

Vulnerability in cURL and libcurl

October 11, 2023 — v1.0

TLP:CLEAR

History:

- *11/10/2023 — v1.0 – Initial publication*

Summary

A security vulnerability in the cURL tool and libcurl library has been identified [1]. This flaw enables a heap-based buffer overflow during the SOCKS5 proxy handshake, potentially allowing malicious actors to execute arbitrary code (RCE). At this time, CERT-EU is not aware of any active exploits leveraging this vulnerability. The vulnerability affects libcurl versions 7.69.0 to 8.3.0. The issue was reported on September 30, 2023, and a patch has been released in curl version 8.4.0. The vulnerability is tracked as `CVE-2023-38545`.

Technical Details

The vulnerability arises from a bug in curl's handling of hostnames during the SOCKS5 proxy handshake. When instructed to forward the hostname to the SOCKS5 proxy for resolution, curl has a maximum limit of 255 bytes. If a hostname longer than this is encountered, a bug may cause the program to mistakenly copy the entire hostname to the target buffer, instead of just the resolved address.

For the vulnerability to be exploitable, the application must use `socks5h` proxy as described below.

In libcurl : - `CURLOPT_PROXYTYPE` set to type `CURLPROXY_SOCKS5_HOSTNAME`, or: - `CURLOPT_PROXY` or `CURLOPT_PRE_PROXY` set to use the scheme `socks5h://` - One of the proxy environment variables can be set to use the `socks5h://` scheme. For example `http_proxy`, `HTTPS_PROXY` or `ALL_PROXY`.

In cURL tool : - `--socks5-hostname`, or: - `--proxy` or `--preproxy` set to use the scheme `socks5h://` - Environment variables as described in the libcurl section.

It also requires that the victim access an attacker controlled website.

Affected Products

- libcurl to 7.69.0 to 8.3.0

Note: Versions prior to 7.69.0 are **not affected**.

Recommendations

While CERT-EU assess the exploitability of this vulnerability as low, CERT-EU recommends updating to cURL 8.4.0.

As cURL and libcurl are being used by a large variety of operating systems and applications, CERT-EU recommends prioritising the patching on public facing applications, and especially those accepting arbitrary user inputs, and critical systems.

References

[1] https://curl.se/docs/CVE-2023-38545.html