CVE-2020-8284

Awarded 700 USD

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

trusting FTP PASV responses

Project curl Security Advisory, December 9 2020
Permalink

VULNERABILITY

When curl performs a passive FTP transfer, it first tries the `EPSV` command and if that is not supported, it falls back to using `PASV`. Passive mode is what curl uses by default.

A server response to a `PASV` command includes the (IPv4) address and port number for the client to connect back to in order to perform the actual data transfer.

This is how the FTP protocol is designed to work.

A malicious server can use the `PASV` response to trick curl into connecting back to a given IP address and port, and this way potentially make curl extract information about services that are otherwise private and not disclosed, for example doing port scanning and service banner extractions.

If curl operates on a URL provided by a user (which by all means is an unwise setup), a user can exploit that and pass in a URL to a malicious FTP server instance without needing any server breach to perform the attack.

INFO

This issue has existed in curl for as long as FTP has been supported, since day 1.

The flaw only exists for IPv4 since `PASV` does not work for IPv6 and curl prefers `EPSV`. The passive mode setup for FTP is used for both uploads and downloads.

curl can be built without FTP support and applications can explicitly disable FTP for single transfers.

curl users could already mitigate this flaw with `CURLOPT_FTP_SKIP_PASV_IP` and `--ftp-skip-pasv-ip`.

Other FTP clients have in the past also had this flaw and have fixed it at different points in time. Firefox fixed it in 2007: CVE-2007-1562.

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2020-8284 to this issue.

CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Severity: Low

AFFECTED VERSIONS

- Affected versions: curl 4.0 to and including 7.73.0
- Not affected versions: curl >= 7.74.0
- Introduced-in: https://github.com/curl/curl/commit/ae1912cb0d494b48d

Also note that (lib)curl is used by many applications, and not always advertised as such.

SOLUTION

The IP address part of the response is now ignored by default, by making `CURLOPT_FTP_SKIP_PASV_IP` default to `1L` instead of previously being `0L`.

This has the minor drawback that a small fraction of use cases might break, when a server truly needs the client to connect back to a different IP address than what the control connection uses and for those `CURLOPT_FTP_SKIP_PASV_IP` can be set to `0L`.

The same goes for the command line tool, which then might need `--no-ftp-skip-pasv-ip` set to prevent curl from ignoring the address in the server response.

- Fixed-in: https://github.com/curl/curl/commit/ec9cc725d598ac

RECOMMENDATIONS

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

A - Upgrade libcurl to version 7.74.0

B - Set `CURLOPT_FTP_SKIP_PASV_IP` to `1L` or use `--ftp-skip-pasv-ip`

C - Disable FTP availability for your transfers

TIMELINE

This issue was first reported to the curl project on November 21, 2020.

This advisory was posted on December 9 2020.

CREDITS

- Reported-by: Varnavas Papaioannou
- Patched-by: Daniel Stenberg

Thanks a lot!