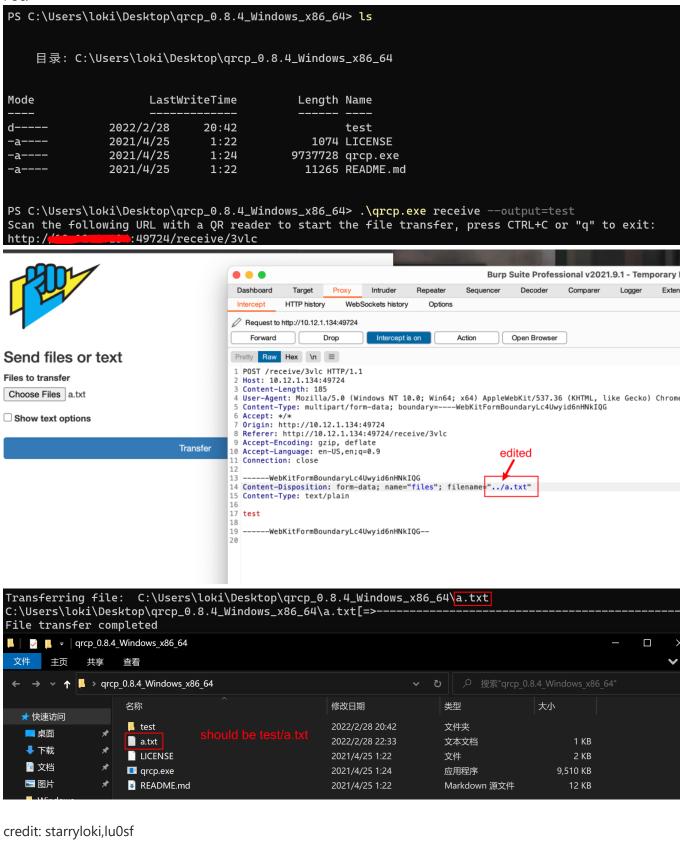


While qrcp works on receive mode, uploader can edit the file name in HTTP request and add "../". Meanwhile, qrcp doesn't check legality of file name which lead to directory traversal.

Env: qrcp-0.8.4, Windows 10 x86_64, Ubuntu 20.04 x86_64

Poc:



Owner

Hello, many thanks for spotting & reporting, I will focus on this very soon.

C

claudiodangelis linked a pull request on Mar 3 that will close this issue

Extract base from multipart #224

№ Merged

claudiodangelis mentioned this issue on Mar 3

Extract base from multipart #224

、 Merged

claudiodangelis closed this as completed in #224 on Mar 3

claudiodangelis commented on Mar 3 • edited •

Owner

This was apparently an issue on the mime/multipart package of Go itself, which has been fixed 10 months ago, a few weeks after the latest release of qrcp.

Links:

- https://go-review.googlesource.com/c/go/+/313809
- golang/go@ 784ef4c

I added a patch, should be all good now, can you please confirm? Thanks

EDIT: patch released as of version 0.8.5.

- **a** claudiodangelis reopened this on Mar 3
- starryloki closed this as completed on Mar 4

Assignees

No one assigned

Labels

. .

None yet
Projects
None yet
Milestone
No milestone
Development
Successfully merging a pull request may close this issue.
Extract base from multipart claudiodangelis/qrcp

2 participants



