Null pointer dereference in httpd.c #346

☑ Closed **Taolaw** opened this issue on May 23 · 2 comments

Taolaw commented on May 23

poc

```
GET /tar/tar.tar/.. HTTP/1.1\r\n\r\n
```

crash scene

```
pwndbg> bt
#0  strstart (a=a@entry=0x7fffffffdb58, b=b@entry=0x0) at lib/lib.c:506
#1  0x00005555555749f4 in isunder (dir=0x5555555bb7d4 ".", file=0x5555555cd535 "tar/tar.tar/..") at t
#2  handle (infd=<optimized out>, outfd=1) at toys/net/httpd.c:132
#3  0x000055555556fcee in toy_exec_which (which=<optimized out>, argv=<optimized out>) at main.c:220
#4  0x000055555556fda1 in toybox_main () at main.c:246
#5  0x000055555556fcee in toy_exec_which (which=<optimized out>, argv=<optimized out>) at main.c:220
#6  0x000055555556fda1 in toybox_main () at main.c:246
#7  0x000055555556675f in main (argc=argc@entry=3, argv=argv@entry=0x7fffffffded8) at main.c:293
#8  0x00007ffff7c8cd90 in __libc_start_call_main (main=main@entry=0x555555566710 <main>, argc=argc@en
#9  0x00007ffff7c8ce40 in __libc_start_main_impl (main=0x555555566710 <main>, argc=3, argv=0x7fffffff
#10 0x0000555555566795 in _start ()
```

Anaylize

It seems that he did not deal with the situation that the return value of `xabspath` was `NULL`, which led to the subsequent dereferencing of this NULL, and continued to trace the location of the `xwrap.c:599` line. When the judgment here is true, it will be Return NULL. I think this error is a code path that may not be considered. But appearing in the `httpd` remote service may cause a remote denial of service.

discoverer

Taolaw@Vlab Team of Vecentek

landley commented on May 29 Owner

Commit 6d48479

landley commented on Jun 9 Owner

I'm assuming in the absence of a reply that commit fixed it for you.

landley closed this as completed on Jun 9

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants