New issue

Jump to bottom

Potential memory corruption/crash due to overlapping strcpy arguments #14

Open jasperla opened this issue on Jan 26, 2021 · 1 comment

jasperla commented on Jan 26, 2021

When building sthttpd with ASAN (`-fsanitize=address`) I noticed a number of crashes with trivial requests such as the following:

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

The problem is most visible on systems where `strcpy` is implemented using `memcpy` (e.g. GLIBC and macOS), here we end up with `memcpy` on overlapping memory ranges:

```
% ./thttpd.asan -p 8080  -d www -D -l -
=================================================================
==3926288==ERROR: AddressSanitizer: strcpy-param-overlap: memory ranges [0x611000000180,0x611000000189) and [0x611000000184, 0x61100000018d) overlap
    #0 0x4850ba in strcpy (/home/jasper/sthttpd/thttpd.asan+0x4850ba)
    #1 0x4d5532 in de_dotdot /home/jasper/sthttpd/src/libhttpd.c:2425:9
    #2 0x4d3961 in httpd_parse_request /home/jasper/sthttpd/src/libhttpd.c:2040:5
    #3 0x4cce31 in handle_read /home/jasper/sthttpd/src/thttpd.c:1646:10
    #4 0x4c9fa0 in main /home/jasper/sthttpd/src/thttpd.c:809:26
    #5 0x7f7c99f75d09 in __libc_start_main csu/../csu/libc-start.c:308:16
    #6 0x41f569 in _start (/home/jasper/sthttpd/thttpd.asan+0x41f569)

0x611000000180 is located 0 bytes inside of 201-byte region [0x611000000180,0x611000000249)
allocated by thread T0 here:
    #0 0x4995dd in malloc (/home/jasper/sthttpd/thttpd.asan+0x4995dd)
    #1 0x4d162e in httpd_realloc_str /home/jasper/sthttpd/src/libhttpd.c:701:10
    #2 0x4cc4e0 in handle_newconnect /home/jasper/sthttpd/src/thttpd.c:1550:11

0x611000000184 is located 4 bytes inside of 201-byte region [0x611000000180,0x611000000249)
allocated by thread T0 here:
    #0 0x4995dd in malloc (/home/jasper/sthttpd/thttpd.asan+0x4995dd)
    #1 0x4d162e in httpd_realloc_str /home/jasper/sthttpd/src/libhttpd.c:701:10
    #2 0x4cc4e0 in handle_newconnect /home/jasper/sthttpd/src/thttpd.c:1550:11

SUMMARY: AddressSanitizer: strcpy-param-overlap (/home/jasper/sthttpd/thttpd.asan+0x4850ba) in strcpy
==3926288==ABORTING
```

Regardless of whether the server crashes, the behaviour of `strcpy` with overlapping source and destination is warned against in the manpage as the resulting behaviour is undefined. As the trace above shows, the offending call happens from https://github.com/blueness/sthttpd/blob/master/src/libhttpd.c#L2406

jasperla commented on Feb 8, 2021 Author

This was assigned CVE-2021-26843.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant