

New issue

Jump to bottom

A Buffer Overflow Write Bug at Checksum.c:88 #556

Closed

lvtao-sec opened this issue on May 7, 2019 · 2 comments

Labels bug
Projects 4.3.3

lvtao-sec commented on May 7, 2019 • edited

Describe the bug

There is a buffer overflow write at checksum.c:88 , download at latest commit a00fd47 .

Code near checksum.c:88 is showed below.

The code didn't check whether the data is long enough comparing IP and TCP packet length. When running the poc, the data len is even less than IP header. So a buffer overflow write will reported when writing to TCP header.

```
37 do_checksum(tcpedit_t *tcpedit, uint8_t *data, int proto, int len) {  
...  
ip_hl = //assign value to ip_hl  
...  
80 switch (proto) {  
81  
82 case IPPROTO_TCP:  
83 tcp = (tcp_hdr_t *) (data + ip_hl); //note: A check patch should be here  
84 #ifdef STUPID_SOLARIS_CHECKSUM_BUG  
85 tcp->th_sum = tcp->th_off << 2;  
86 return (TCPEDIT_OK);  
87 #endif  
88 tcp->th_sum = 0; //Buffer overflow write occurs here.
```

To Reproduce

Steps to reproduce the behavior:

1. download the code from commit a00fd47 (master head now).
2. download poc
3. Compile program with CFLAGS="-g -O0 -fsanitize=address"
4. Execute tcpreplay-edit -r 80:84 -s 20 -b -C -m 1500 -P --oneatime -i eth0 \$poc

Expected behavior


A buffer overflow write will be reported by ASAN, which is showed at below screen shots part.

Screenshots

```
$ gdb -q -arg tcpreplay-edit -r 80:84 -s 20 -b -C -m 1500 -P --oneatime -i eth0 ./poc  
Reading symbols from /home/lt/vuln-fuzz/program/tcpreplay/asan-install/bin/tcpreplay-edit...done.  
(gdb) b checksum.c:83  
Breakpoint 1 at 0x427dee: file checksum.c, line 83.  
(gdb) r  
Starting program: /home/lt/vuln-fuzz/program/tcpreplay/asan-install/bin/tcpreplay-edit -r 80:84 -s 20 -b -C -m 1500 -P --oneatime -i eth0  
crashes/id:000004,sig:06,src:000008+000292,op:splice,rep:2  
[Thread debugging using libthread_db enabled]  
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".  
PID: 65942  
Warning: crashes/id:000004,sig:06,src:000008+000292,op:splice,rep:2 was captured using a snaplen of 64 bytes. This may mean you have truncated packets.  
  
Breakpoint 1, do_checksum (tcpedit=0x61d0001e000, data=0x60600000ec0e "[", proto=6, len=4) at checksum.c:83  
83 tcp = (tcp_hdr_t *) (data + ip_hl);  
(gdb) p len  
$1 = 4  
(gdb) p ip_hl  
$2 = 44  
(gdb) n  
88 tcp->th_sum = 0;  
(gdb) p *tcp  
$3 = {th_sport = 8738, th_dport = 8738, th_seq = 2528755390, th_ack = 52334, th_x2 = 0 '\000', th_off = 0 '\000',  
th_flags = 0 '\000', th_win = 60496, th_sum = 0, th_urp = 24672}  
(gdb) n  
=====  
==65942==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60600000ec4a at pc 0x000000427e3a bp 0x7fffffff660 sp 0x7fffffff650  
WRITE of size 2 at 0x60600000ec4a thread T0  
#0 0x427e39 in do_checksum /home/lt/vuln-fuzz/program/tcpreplay/src/tcpedit/checksum.c:88  
#1 0x41f0ca in fix_ipv4_checksums /home/lt/vuln-fuzz/program/tcpreplay/src/tcpedit/edit_packet.c:74  
#2 0x41c209 in tcpedit_packet /home/lt/vuln-fuzz/program/tcpreplay/src/tcpedit/tcpedit.c:354  
#3 0x408f4b in send_packets /home/lt/vuln-fuzz/program/tcpreplay/src/send_packets.c:552  
#4 0x4187aa in replay_file /home/lt/vuln-fuzz/program/tcpreplay/src/replay.c:182  
#5 0x417783 in tcpr_replay_index /home/lt/vuln-fuzz/program/tcpreplay/src/replay.c:59  
#6 0x4166f4 in tcpreplay_replay /home/lt/vuln-fuzz/program/tcpreplay/src/tcpreplay_api.c:1136  
#7 0x40f45f in main /home/lt/vuln-fuzz/program/tcpreplay/src/tcpreplay.c:139  
#8 0x7ffff665d82f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)  
#9 0x402e18 in _start (/home/lt/vuln-fuzz/program/tcpreplay/asan-install/bin/tcpreplay-edit+0x402e18)  
  
0x60600000ec4a is located 10 bytes to the right of 64-byte region [0x60600000ec00,0x60600000ec40)  
allocated by thread T0 here:  
#0 0x7ffff6f02602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98602)  
#1 0x7ffff6c4752e (/usr/lib/x86_64-linux-gnu/libc.so.6+0x1f52e)  
  
SUMMARY: AddressSanitizer: heap-buffer-overflow /home/lt/vuln-fuzz/program/tcpreplay/src/tcpedit/checksum.c:88 do_checksum  
Shadow bytes around the buggy address:  
0x0c0c7fff9d30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa  
0x0c0c7fff9d40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa  
0x0c0c7fff9d50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa  
0x0c0c7fff9d60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

```
0x0c8c7fff9d70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c8c7fff9d80: 00 00 00 00 00 00 00 00 fa[fa]fa fa 00 00 00 00
0x0c8c7fff9d90: 00 00 00 03 fa fa fa fa fd fd fd fd fd fd fd fd
0x0c8c7fff9da0: fa fa fa fa fd fd fd fd fd fd fd fd fd fa fa fa
0x0c8c7fff9db0: 00 00 00 00 00 00 00 00 fa fa fa fa fd fd fd fd
0x0c8c7fff9dc0: fd fd fd fd fa fa fa fa fd fd fd fd fd fd fd fd
0x0c8c7fff9dd0: fa fa fa fa fd fd fd fd fd fd fd fd fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
Addressable: 00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone: fa
Heap right redzone: fb
Freed heap region: fd
Stack left redzone: f1
Stack mid redzone: f2
Stack right redzone: f3
Stack partial redzone: f4
Stack after return: f5
Stack use after scope: f8
Global redzone: f9
Global init order: f6
Poisoned by user: f7
Container overflow: fc
Array cookie: ac
Intra object redzone: bb
ASAN internal: fe
==65942==ABORTING
[Inferior 1 (process 65942) exited with code 01]
```

System (please complete the following information):

- OS: ubuntu linux
- OS version : 4.2.0-16-generic  option --unique-ip is slower than expected. #19-Ubuntu SMP Thu Oct 8 15:35:06 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
- Tcpreplay Version : master head at 2019-05-07 commit [a00fd47](#)

  **lvtao-sec** changed the title ~~(Bug)~~ A Buffer Overflow Write Bug at Checksum.c:88 on May 7, 2019

lvtao-sec commented on May 7, 2019 • edited 

Author

This bug is different from this issue [#538](#).

 **GabrielGanne** added a commit to GabrielGanne/tcpreplay that referenced this issue on May 9, 2019

 fix do_checksum() packet dissection ...

69ad4bd

  **fklassen** added the bug label on May 9, 2019

  **fklassen** added this to To do in 4.3.3 via  on May 9, 2019

  **14isnot40** mentioned this issue on May 19, 2020

[Bug] tcpreplay-edit — heap-buffer-overflow in do_checksum at Checksum.c:132 #577

 Closed

  **fklassen** moved this from To do to In progress in 4.3.3 on Jun 1, 2020

 **fklassen** added a commit that referenced this issue on Jun 1, 2020

 Bug [#556](#) [#538](#) guard HBO in checksum - fix as per [@Gabrie1Ganne](#)

f3fe91f

 **fklassen** added a commit that referenced this issue on Jun 1, 2020


 Merge pull request [#591](#) from appneta/Bug_#556_#538_heap-buffer-overf1...

b763db7


fklassen commented on Jun 1, 2020

Member

Fixed as per [@Gabrie1Ganne](#) patch in [#591](#)

 **fklassen** closed this as completed on Jun 1, 2020

 4.3.3  moved this from In progress to Done on Jun 1, 2020

 **fklassen** added a commit that referenced this issue on Jun 2, 2020

 Bug [#556](#) fix build warning

e1cec77

 **fklassen** added a commit that referenced this issue on Jun 2, 2020

 Merge pull request [#592](#) from appneta/Bug_#556_#538_correct_warning ...

34b456d

Assignees

No one assigned

Labels

bug

Projects

No open projects

1 closed project ▾

Milestone

No milestone

Development

No branches or pull requests

2 participants

