New issue

Jump to bottom

A global-buffer-overflow in hcxpcapngtool.c:3789:4 #155

Closed **seviezhou** opened this issue on Aug 11, 2020 · 7 comments

seviezhou commented on Aug 11, 2020 • edited

System info

Ubuntu x86_64, clang 6.0, hcxpcapngtool (latest master e6b738)

Configure

CFLAGS="-g -fsanitize=address" LDFLAGS="-fsanitize=address" make

Command line

./hcxpcapngtool --all -o /dev/null @@

AddressSanitizer output

```
=================================================================
==24965==ERROR: AddressSanitizer: global-buffer-overflow on address 0x00000149db60 at pc 0x0000004ddcc5 bp 0x7ffffd559690 sp 0x7ffffd558e40
WRITE of size 1536 at 0x00000149db60 thread T0
    #0 0x4ddcc4 in __asan_memcpy /home/seviezhou/llvm-6.0.0/projects/compiler-rt/lib/asan/asan_interceptors_memintrinsics.cc:23
    #1 0x522c14 in pcapngoptionwalk /home/seviezhou/hcxtools/hcxpcapngtool.c:3789:4
    #2 0x5247d1 in processpcapng /home/seviezhou/hcxtools/hcxpcapngtool.c:4083:3
    #3 0x526c36 in processcapfile /home/seviezhou/hcxtools/hcxpcapngtool.c:4191:3
    #4 0x526c36 in main /home/seviezhou/hcxtools/hcxpcapngtool.c:4896
    #5 0x7f973984483f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
    #6 0x41ab58 in _start (/home/seviezhou/hcxtools/hcxpcapngtool+0x41ab58)

0x00000149db60 is located 0 bytes to the right of global variable 'nmeasentence' defined in 'hcxpcapngtool.c:284:13' (0x149d760) of size 1024
SUMMARY: AddressSanitizer: global-buffer-overflow /home/seviezhou/llvm-6.0.0/projects/compiler-rt/lib/asan/asan_interceptors_memintrinsics.cc:23 in __asan_memcpy
Shadow bytes around the buggy address:
  0x00008028bb10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x00008028bb20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x00008028bb30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x00008028bb40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x00008028bb50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x00008028bb60: 00 00 00 00 00 00 00 00 00 00 00 00[f9]f9 f9 f9
  0x00008028bb70: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x00008028bb80: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 00 f9 f9 f9
  0x00008028bb90: f9 f9 f9 f9 00 f9 f9 f9 f9 f9 f9 f9 00 f9 f9 f9
  0x00008028bba0: f9 f9 f9 f9 04 f9 f9 f9 f9 f9 f9 f9 04 f9 f9 f9
  0x00008028bbb0: f9 f9 f9 f9 04 f9 f9 f9 f9 f9 f9 f9 00 f9 f9 f9
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
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  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
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==24965==ABORTING
```

POC

global-overflow-pcapngoptionwalk-hcxpcapngtool-3789.zip

seviezhou changed the title ~~A memcpy-param-overlap in hcxpcapngtool.c:3789:4~~ **A global-buffer-overflow in hcxpcapngtool.c:3789:4** on Aug 11, 2020

ZerBea commented on Aug 12, 2020 • edited Owner

Thanks for reporting that issue. It should be fixed by latest commit:
e6505dd

Analysis of the attached pcapng file:
The dumpfile contain 4 IPv4 UDP frames.
Frame 4 is damaged (Wireshark/tshark will not show frame 4).

```
$ tshark -r memcpy-param-overlap-pcapngoptionwalk-hcxpcapngtool-3786
    1 05:44:20,095111 172.16.98.182 → 172.16.98.2  DNS 70 Standard query 0xee40 A domain.xyz
    2 05:44:20,096318  172.16.98.1 → 172.16.98.105 DNS 70 Standard query 0xee40 A domain.xyz
```

```
    3 05:44:20,096678 172.16.98.105 → 172.16.98.1  DNS 124 Standard query response 0xee40 A domain.xyz SOA 1856329112e5

tshark: The file "memcpy-param-overlap-pcapngoptionwalk-hcxpcapngtool-3786" appears to be damaged or corrupt.
(pcapng_read_option: Not enough data to handle option length (32768) of the packet block)
```

By latest commit, hcxpcangtool is able to handle that kind of damaged pcapng files (inclusive detection of all included frames):

```
$ hcxpcapngtool memcpy-param-overlap-pcapngoptionwalk-hcxpcapngtool-3786
reading from memcpy-param-overlap-pcapngoptionwalk-hcxpcapngtool-3786...
failed to read pcapng block header

summary capture file
--------------------
file name.............................: memcpy-param-overlap-pcapngoptionwalk-hcxpcapngtool-3786
version (pcapng)......................: 1.0
operating system......................: N/A
application...........................: N/A
interface name........................: vmnet8
interface vendor......................: 000000
weak candidate........................: N/A
MAC ACCESS POINT......................: 000000000000 (incremented on every new client)
MAC CLIENT............................: 000000000000
REPLAYCOUNT...........................: 0
ANONCE................................: 0000000000000000000000000000000000000000000000000000000000000000
SNONCE................................: 0000000000000000000000000000000000000000000000000000000000000000
timestamp minimum (GMT)...............: 13.05.2016 07:44:20
timestamp maximum (GMT)...............: 13.05.2016 07:44:20
used capture interfaces...............: 1
link layer header type................: DLT_EN10MB (1)
endianess (capture system)............: little endian
packets inside........................: 4
IPv4..................................: 4
UDP...................................: 4
EAPOL ANONCE error corrections (NC)...: not detected
packet read error.....................: 1

Warning: missing frames!
This dump file contains no undirected proberequest frames.
An undirected proberequest may contain information about the PSK.
It always happens if the capture file was cleaned or
it could happen if filter options are used during capturing.
That makes it hard to recover the PSK.

Warning: missing frames!
This dump file contains no important frames like
authentication, association or reassociation.
It always happens if the capture file was cleaned or
it could happen if filter options are used during capturing.
That makes it hard to recover the PSK.

Warning: missing frames!
This dump file doesn't contain enough EAPOL M1 frames.
It always happens if the capture file was cleaned or
it could happen if filter options are used during capturing.
That makes it impossible to calculate nonce-error-correction values.
```

Please test and reopen issue, if it doesn't work for you.

👍 1

ZerBea closed this as completed on Aug 12, 2020

---

seviezhou commented on Aug 12, 2020 — Author

I think this commit has fixed this issue.

ZerBea commented on Aug 12, 2020 — Owner

The attached pcapng file is very appreciated and helped to improve hcxtools.
Now, 4 frames detected by hcxpcangtool vs 3 frames detected by tshark/Wireshark.

seviezhou commented on Aug 12, 2020 — Author

Glad that it helps.

fgeek commented on Sep 21, 2021

CVE-2021-32286 has been assigned for this issue.

ZerBea commented on Sep 21, 2021 — Owner

And it was fixed a long time ago.

```
$ valgrind hcxpcapngtool -o test.22000 global-overflow-pcapngoptionwalk-hcxpcapngtool-3789.pcpng
hcxpcapngtool 6.2.4-8-gaaa4238 reading from global-overflow-pcapngoptionwalk-hcxpcapngtool-3789.pcpng...
failed to read pcapng block header

summary capture file
--------------------
file name.............................: global-overflow-pcapngoptionwalk-hcxpcapngtool-3789.pcpng
version (pcapng)......................: 1.0
operating system......................: N/A
application...........................: N/A
interface name........................: vmnet8
interface vendor......................: 000000
```

```
openSSL version.........................: 1.1
weak candidate..........................: N/A
MAC ACCESS POINT........................: 000000000000 (incremented on every new client)
MAC CLIENT..............................: 000000000000
REPLAYCOUNT.............................: 0
ANONCE..................................: 0000000000000000000000000000000000000000000000000000000000000000
SNONCE..................................: 0000000000000000000000000000000000000000000000000000000000000000
timestamp minimum (GMT).................: 13.05.2016 07:44:20
timestamp maximum (GMT).................: 13.05.2016 07:44:20
used capture interfaces.................: 1
link layer header type..................: DLT_EN10MB (1)
endianess (capture system)..............: little endian
packets inside..........................: 4
IPv4 (total)............................: 3
UDP (total).............................: 3
EAPOL ANONCE error corrections (NC).....: not detected
packet read error.......................: 2

Information: no hashes written to hash files

Warning: missing frames!
This dump file does not contain undirected proberequest frames.
An undirected proberequest may contain information about the PSK.
It always happens if the capture file was cleaned or
it could happen if filter options are used during capturing.
That makes it hard to recover the PSK.

Warning: missing frames!
This dump file does not contain important frames like
authentication, association or reassociation.
It always happens if the capture file was cleaned or
it could happen if filter options are used during capturing.
That makes it hard to recover the PSK.

Warning: missing frames!
This dump file does not contain enough EAPOL M1 frames.
It always happens if the capture file was cleaned or
it could happen if filter options are used during capturing.
That makes it impossible to calculate nonce-error-correction values.


session summary
---------------
processed pcapng files.................: 1

==32397== Memcheck, a memory error detector
==32397== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==32397== Using Valgrind-3.17.0 and LibVEX; rerun with -h for copyright info
==32397== Command: hcxpcapngtool -o test.22000 global-overflow-pcapngoptionwalk-hcxpcapngtool-3789.pcpng
==32397== HEAP SUMMARY:
==32397==     in use at exit: 0 bytes in 0 blocks
==32397==   total heap usage: 0 allocs, 0 frees, 0 bytes allocated
==32397==
==32397== All heap blocks were freed -- no leaks are possible
==32397==
==32397== For lists of detected and suppressed errors, rerun with: -s
==32397== ERROR SUMMARY: 0 errors from 0 contexts (suppressed: 0 from 0)
```

ZerBea commented on Sep 21, 2021 — Owner

@fgeek , but anyway, your comment reminded me that I forgot to make a changelog entry that it was fixed.
Now done by this commit:
6f77455
Thanks.

👍 1

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants