New issue

Jump to bottom

[BUG] out of bound write in checkType, etc.c:441 #242

Open kdsjZh opened this issue on Aug 7 · 11 comments

kdsjZh commented on Aug 7 • edited

Hello, I found a out of bound write in w3m, function checkType, etc.c:441 while testing my new fuzzer.

step to reproduce

```
export CC="gcc -fsanitize=address -g" ./configure --disable-shared && make -j8
./w3m $POC
```

Environment

- Ubuntu 22.04 (docker image)
- w3m latest commit `c515ea8`
- gcc 11.2.0

ASan log

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==1795279==ERROR: AddressSanitizer: BUS on unknown address (pc 0x5639811267b7 bp 0x7f4212857ffe sp
0x7ffdc528ad90 T0)
==1795279==The signal is caused by a WRITE memory access.
==1795279==Hint: this fault was caused by a dereference of a high value address (see register
values below).  Dissassemble the provided pc to learn which register was used.
    #0 0x5639811267b7 in checkType /validate/w3m/etc.c:441
    #1 0x5639810ea5e2 in loadBuffer /validate/w3m/file.c:7717
    #2 0x563981110094 in loadSomething /validate/w3m/file.c:230
    #3 0x563981110094 in loadGeneralFile /validate/w3m/file.c:2286
    #4 0x5639810ab87d in main /validate/w3m/main.c:1053
    #5 0x7f42159b4d8f in __libc_start_call_main ../sysdeps/nptl/libc_start_call_main.h:58
    #6 0x7f42159b4e3f in __libc_start_main_impl ../csu/libc-start.c:392
    #7 0x5639810af284 in _start (/validate/w3m/w3m+0xb3284)
```

```
AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: BUS /validate/w3m/etc.c:441 in checkType
==1795279==ABORTING
```

Credit

Han Zheng
NCNIPC of China
Hexhive

POC

poc0.zip

rkta commented on Aug 9 — Contributor

> On Sun, Aug 07, 2022 at 04:27:40AM -0700, Han Zheng wrote:
> Hello, I found a out of bound write in w3m, function checkType, etc.c:441 while testing my new fuzzer.
>
> ## step to reproduce
> export CC="gcc -fsanitize=address -g" ./configure --disable-shared && make -j8
> ./w3m $POC

Can't reproduce on Debian with the 'poc0' from the attached zip file.

kdsjZh commented on Aug 9 — Author

Sorry, I write the wrong command, the command is `./w3m -dump $POC` .

kdsjZh commented on Aug 9 • edited — Author

if it didn't work, could you try docker ubuntu 22.04 image with following command? Or you could give me the debian version you use

```
apt update && apt install wget git unzip gcc g++ make libgc-dev libtinfo-dev -y
git clone https://github.com/tats/w3m && pushd w3m
export CC="gcc -fsanitize=address -g" && ./configure --disable-shared && make -j8
./w3m -dump $PATH_TO_POC
```

I try again and it works for me.

rkta commented on Aug 9 — Contributor

> On Tue, Aug 09, 2022 at 07:55:19AM -0700, Han Zheng wrote:
> if it didn't work,

Can not reproduce with '-dump' either.

> could you try ubuntu 22.04 image with following
> command?

I currently don't have time to setup a VM, maybe at the weekend, sorry.

> Or you could give me the debian version you use

Debian stable

> ```
> apt update && apt install wget git unzip gcc g++ make libgc-dev libtinfo-dev -y
> git clone https://github.com/tats/w3m && pushd w3m
> export CC="gcc -fsanitize=address -g" && ./configure --disable-shared && make -j8
> ./w3m -dump $PATH_TO_POC
>
> ```
> I try again and it works for me.

Can you reduce the input file? Does it also reproduce with only the
first half or the second half?

kdsjZh commented on Aug 9 • edited — Author

I try debian stable in docker image and it still works.

> I currently don't have time to setup a VM, maybe at the weekend, sorry.

I mean you can install docker in your debian and copy following command :

```
docker pull ubuntu:22.04 && docker run -it ubuntu:22.04 bash
## now step into the container
apt update && apt install wget git unzip gcc g++ make libgc-dev libtinfo-dev -y
git clone https://github.com/tats/w3m && pushd w3m
export CC="gcc -fsanitize=address -g" && ./configure --disable-shared && make -j8
wget https://github.com/tats/w3m/files/9276657/poc0.zip && unzip poc0.zip
./w3m -dump ./poc0
```

Pls told me if it's still not available. I could try to reduce the input file later. But I guess it's environment's fault.

rkta commented on Aug 10 — Contributor

> On Tue, Aug 09, 2022 at 08:36:15AM -0700, Han Zheng wrote:
> I try debian stable in docker image and it still works.

I wonder if Docker plays a role here.

> > I currently don't have time to setup a VM, maybe at the weekend, sorry.
> I mean install docker in your debian and copy following command :
> ```
> docker pull ubuntu:22.04 && docker run -it ubuntu:22.04 bash
> ## now step into the container
> apt update && apt install wget git unzip gcc g++ make libgc-dev libtinfo-dev -y
> git clone https://github.com/tats/w3m && pushd w3m
> export CC="gcc -fsanitize=address -g" && ./configure --disable-shared && make -j8
> wget https://github.com/tats/w3m/files/9276657/poc0.zip && unzip poc0.zip
> ./w3m -dump ./poc0
>
> ```
>
> Pls told me if it's still not available.

Yes, can reproduce this way.

> I could try to reduce the input file later.

Works:
head -c 9215 poc0 | ./w3m -dump

Does not work:
tail -c 9215 poc0 | ./w3m -dump
head -c 9216 poc0 | tail -c 9215 | ./w3m -dump

kdsjZh commented on Aug 10 • edited — Author

I guess it's not docker. I try to reproduce it in my psychical Desktop (ubuntu 21.10) and success with following command

```
./w3m -dump
crashes/id\:000001\,sig\:11\,src\:000876\,time\:8063946\,execs\:818201\,op\:MOpt_core_havoc\,rep\:8

AddressSanitizer:DEADLYSIGNAL
=================================================================
```

```
==3904622==ERROR: AddressSanitizer: SEGV on unknown address 0x7f186ce09ffe (pc 0x55c246d22787 bp
0x7f186ce09ffe sp 0x7ffe334beb20 T0)
==3904622==The signal is caused by a WRITE memory access.
    #0 0x55c246d22787 in checkType /home/kdsj/workspace/benchmarks/reproduce/w3m/etc.c:441
    #1 0x55c246ce65c2 in loadBuffer /home/kdsj/workspace/benchmarks/reproduce/w3m/file.c:7717
    #2 0x55c246d0c074 in loadSomething /home/kdsj/workspace/benchmarks/reproduce/w3m/file.c:230
    #3 0x55c246d0c074 in loadGeneralFile /home/kdsj/workspace/benchmarks/reproduce/w3m/file.c:2286
    #4 0x55c246ca785d in main /home/kdsj/workspace/benchmarks/reproduce/w3m/main.c:1053
    #5 0x7f186fc77fcf in __libc_start_call_main ../sysdeps/nptl/libc_start_call_main.h:58
    #6 0x7f186fc7807c in __libc_start_main_impl ../csu/libc-start.c:409
    #7 0x55c246cab264 in _start (/home/kdsj/workspace/benchmarks/reproduce/w3m/w3m+0xb3264)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/kdsj/workspace/benchmarks/reproduce/w3m/etc.c:441 in
checkType
==3904622==ABORTING
```

but when try to rename it to `poc0`, it failed

```
./w3m -dump crashes/poc0
        ??????????p???�???*��?&?*?p???�???     ?????????????????????????????
```

Although I check again and make sure they're the same crash with same hash....
I guess the name is to be blamed? or there might be some random factor?

N-R-K commented on Aug 15 • edited — Contributor

@kdsjZh Hi, could you please provide the output of `./w3m -version`, I'm not able to reproduce on my system. And the suspect code snippet is filled with various `#ifdefs` so it might be related to a specific configuration.

P.S: `--disable-shared` doesn't seem to be a valid option and gives me the following warning on `master`:

```
configure: WARNING: unrecognized options: --disable-shared
```

N-R-K commented on Aug 15 — Contributor

Also since I'm not able to reproduce on my end, please also check if the following patch fixes the issue or not:

```
diff --git a/etc.c b/etc.c
index 805bfa0..bbad19c 100644
--- a/etc.c
```

```
+++ b/etc.c
@@ -438,12 +438,13 @@ checkType(Str s, Lineprop **oprop, Linecolor **ocolor)
            mode |= ceffect;
        }
 #endif
-       *(prop++) = mode;
+       if (prop < prop_buffer + prop_size)
+               *(prop++) = mode;
 #ifdef USE_M17N
        plen = get_mclen(str);
        if (plen > 1) {
            mode = (mode & ~PC_WCHAR1) | PC_WCHAR2;
-           for (i = 1; i < plen; i++) {
+           for (i = 1; i < plen && prop < prop_buffer + prop_size; i++) {
                *(prop++) = mode;
 #ifdef USE_ANSI_COLOR
                if (color)
```

kdsjZh commented on Aug 16 — Author

> could you please provide the output of ./w3m -version

```
./w3m --version
w3m version w3m/0.5.3+git20220429, options lang=en,m17n,image,color,ansi-
color,mouse,menu,cookie,external-uri-loader,w3mmailer,nntp,gopher,ipv6,alarm,mark
```

> P.S: --disable-shared doesn't seem to be a valid option and gives me the following warning on master:

Sorry, this is a typo, you can remove this arg.

> check if the following patch fixes the issue or not:

It seems not. I try to use gdb and it shows that pointer prop itself is valid.

```
gdb-peda$ set args -dump poc0
gdb-peda$ r
Starting program: /home/kdsj/workspace/fuzz/verify/w3m/w3m -dump poc0
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
[New Thread 0x7ffff3dff640 (LWP 331510)]
[New Thread 0x7ffff35fe640 (LWP 331511)]
[New Thread 0x7ffff2dfd640 (LWP 331512)]
[New Thread 0x7ffff25fc640 (LWP 331513)]
[New Thread 0x7ffff1dfb640 (LWP 331514)]
[New Thread 0x7ffff15fa640 (LWP 331515)]
[New Thread 0x7ffff0df9640 (LWP 331516)]
[New Thread 0x7ffff05f8640 (LWP 331517)]
[New Thread 0x7fffefdf7640 (LWP 331518)]
[New Thread 0x7fffef5f6640 (LWP 331519)]
[New Thread 0x7fffeedf5640 (LWP 331520)]
```

```
Thread 1 "w3m" received signal SIGSEGV, Segmentation fault.
[----------------------------------registers-----------------------------------]
RAX: 0x7
RBX: 0x7ffff441cc5a --> 0x808080808080808
RCX: 0x0
RDX: 0x1200
RSI: 0x7ffff4404000 --> 0x100000001000100
RDI: 0x5555558d9a85 --> 0x200a020a020a0212
RBP: 0x7ffff4403ffe
RSP: 0x7fffffffd720 --> 0x0
RIP: 0x55555567e7bb (<checkType+1403>:  mov    WORD PTR [rbp+0x0],dx)
R8 : 0x7ffff4404000 --> 0x100000001000100
R9 : 0x0
R10: 0x555555754e40 --> 0x5f5f08
R11: 0x2
R12: 0x7ffff441cc57 --> 0x808080808e88085
R13: 0x0
R14: 0x5fca
R15: 0x0
EFLAGS: 0x10246 (carry PARITY adjust ZERO sign trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
   0x55555567e7b1 <checkType+1393>:     jl     0x55555567e7bb <checkType+1403>
   0x55555567e7b3 <checkType+1395>:     test   cl,cl
   0x55555567e7b5 <checkType+1397>:     jne    0x55555567f4b2 <checkType+4722>
=> 0x55555567e7bb <checkType+1403>:     mov    WORD PTR [rbp+0x0],dx
   0x55555567e7bf <checkType+1407>:     mov    rbp,rsi
   0x55555567e7c2 <checkType+1410>:     mov    rdi,r12
   0x55555567e7c5 <checkType+1413>:     mov    DWORD PTR [rsp+0x18],edx
   0x55555567e7c9 <checkType+1417>:     call   0x55555573a340 <wtf_len1>
[------------------------------------stack-------------------------------------]
0000| 0x7fffffffd720 --> 0x0
0008| 0x7fffffffd728 --> 0x7ffff4420fca --> 0x808080808080000
0016| 0x7fffffffd730 --> 0x7ffff463a900 --> 0x7ffff4410000 --> 0x1b1d001b1b001b00
0024| 0x7fffffffd738 --> 0x7ffff4400000
0032| 0x7fffffffd740 --> 0x0
0040| 0x7fffffffd748 --> 0x39e6470e00000003
0048| 0x7fffffffd750 --> 0x100010000 --> 0x0
0056| 0x7fffffffd758 --> 0x7ffff4404000 --> 0x100000001000100
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
0x000055555567e7bb in checkType (s=<optimized out>, s@entry=0x7ffff463a920,
oprop=oprop@entry=0x7fffffffd8c0, ocolor=ocolor@entry=0x0) at etc.c:442
warning: Source file is more recent than executable.
442                     *(prop++) = mode;
gdb-peda$ display prop
1: prop = (Lineprop *) 0x7ffff4404000
gdb-peda$ display prop_buffer
2: prop_buffer = (Lineprop *) 0x7ffff4404000
gdb-peda$ display prop_size
3: prop_size = 0x5fca
```

> I'm not able to reproduce on my system.

Could you try docker when you're available? Considering that there are many environment factors it's better to start from empty docker image. Sometimes even the crash seed's name matters...

```
docker pull ubuntu:22.04 && docker run -it ubuntu:22.04 bash
## now step into the container
apt update && apt install wget git unzip gcc g++ make libgc-dev libtinfo-dev -y
git clone https://github.com/tats/w3m && pushd w3m
export CC="gcc -fsanitize=address -g" && ./configure --disable-shared && make -j8
wget https://github.com/tats/w3m/files/9276657/poc0.zip && unzip poc0.zip
./w3m -dump ./poc0
```

ismaell commented on Oct 22

At first sight, the `checkType` function is a little bit obscure, what is it supposed to do exactly? can someone comment on the variables and their use?

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants