New issue

Jump to bottom

GPAC-2.0.0 MP4Box: stack overflow with unlimited length and controllable content in smil_parse_time_list #2295

Closed 3 tasks done **xidoo123** opened this issue on Oct 29 · 0 comments

xidoo123 commented on Oct 29

Thanks for reporting your issue. Please make sure these boxes are checked before submitting your issue - thank you!

- [x] I looked for a similar issue and couldn't find any.
- [x] I tried with the latest version of GPAC. Installers available at http://gpac.io/downloads/gpac-nightly-builds/
- [x] I give enough information for contributors to reproduce my issue (meaningful title, github labels, platform and compiler, command-line ...). I can share files anonymously with this dropbox: https://www.mediafire.com/filedrop/filedrop_hosted.php?drop=eec9e058a9486fe4e99c33021481d9e1826ca9dbc242a6cfaab0fe95da5e5d95

Detailed guidelines: http://gpac.io/2013/07/16/how-to-file-a-bug-properly/

Description

A fixed length buffer value_string is allocated in smil_parse_time_list, while in the later memcpy, it doesn't check the length and simply copy content to this buffer, causing overflow.

```
static void smil_parse_time_list(GF_Node *e, GF_List *values, char *begin_or_end_list)
{
        SMIL_Time *value;
        char value_string[500];
        char *str = begin_or_end_list, *tmp;
        u32 len;

        /* get rid of leading spaces */
        while (*str == ' ') str++;

        while (1) {
                tmp = strchr(str, ';');
                if (tmp) len = (u32) (tmp-str);
                else len = (u32) strlen(str);
                memcpy(value_string, str, len);
                while ((len > 0) && (value_string[len - 1] == ' '))
```

Impact

Since the content is absolutely controllable by users, an unlimited length will cause stack overflow, corrupting canary, causing DoS or even Remote Code Execution.

Mitigation

We can just set a length limit to it, making it less than 500 byte.

Reproduce

On Ubuntu 22.04 lts, make with this.

```
./configure --static-bin
make
```

Run the following command with POC.svg.

```
MP4Box -mp4 -sync 0x1000 ./POC.svg
```

You may get a buffer overflow detected error.

```
[Parser] SVG Scene Parsing: ../encode_2-gpac-2.0.0/out/default/crashes/0.svg
*** buffer overflow detected ***: terminated              | (00/100)
Aborted
```

GDB info before crash

```
──────────────────────────────────────────────────[ REGISTERS / show-flags off / show-compact-regs off ]──────────────────────────────────────────────────
 RAX  0x6804
 RBX  0x0
 RCX  0x1f4
 RDX  0x6804
*RDI  0x7fffffff6640 ◂— 0x0
 RSI  0xda20cc ◂— 0xff22802d68353548
 R8   0x0
 R9   0xda08b0 ◂— 0x0
 R10  0xda2050 ◂— 0x1790
 R11  0xd80c00 (main_arena+96) —▸ 0xdabcf0 ◂— 0x0
 R12  0xda08b0 ◂— 0x0
 R13  0x7fffffff6640 ◂— 0x0
 R14  0xda20cc ◂— 0xff22802d68353548
 R15  0xb650c3 ◂— 'wallclock('
 RBP  0x6804
 RSP  0x7fffffff6600 ◂— 0x0
```

```
*RIP  0x4c756b (smil_parse_time_list+123) ←— call   0xadfe30
──────────────────────────────────────────────────────────────────────[ DISASM / x86-64 / set emulate on ]──────────────────────────────────────────────────────────────────────
   0x4c77e2 <smil_parse_time_list+754>    jmp    smil_parse_time_list+110                    <smil_parse_time_list+110>
    ↓
   0x4c755e <smil_parse_time_list+110>    mov    edx, ebp
   0x4c7560 <smil_parse_time_list+112>    mov    ecx, 0x1f4
   0x4c7565 <smil_parse_time_list+117>    mov    rsi, r14
   0x4c7568 <smil_parse_time_list+120>    mov    rdi, r13
 ► 0x4c756b <smil_parse_time_list+123>    call   __memcpy_chk                      <__memcpy_chk>
       dstpp: 0x7fffffff6640 ←— 0x0
       srcpp: 0xda20cc ←— 0xff22802d68353548
       len: 0x6804
       dstlen: 0x1f4
```

Backtrace

```
pwndbg> bt
#0  0x0000000000a84c3c in pthread_kill ()
#1  0x0000000000a640d6 in raise ()
#2  0x0000000000402136 in abort ()
#3  0x0000000000a7b476 in __libc_message ()
#4  0x0000000000adfe2a in __fortify_fail ()
#5  0x0000000000adfc46 in __chk_fail ()
#6  0x00000000004c7570 in smil_parse_time_list ()
#7  0x00000000004c965b in gf_svg_parse_attribute ()
#8  0x0000000000063d178 in svg_node_start ()
#9  0x00000000000463486 in xml_sax_node_start ()
#10 0x0000000000464629 in xml_sax_parse ()
#11 0x0000000000464e63 in xml_sax_read_file.part ()
#12 0x000000000046515e in gf_xml_sax_parse_file ()
#13 0x0000000000063b80a in load_svg_run ()
#14 0x000000000042a5e8 in EncodeFile ()
#15 0x000000000041252c in mp4boxMain ()
#16 0x0000000000a598fa in __libc_start_call_main ()
#17 0x0000000000a5b157 in __libc_start_main_impl ()
#18 0x0000000000402b95 in _start ()
```

Credit

xdchase

POC

POC-bof.zip

jeanlf closed this as completed in 0fc7148 on Nov 4

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant