ezXML Bugs

Status: Beta
Brought to you by: voisine

#25 Null pointer dereference in ezxml_internal_dtd()

Milestone: v1.0 (example)
Status: open
Owner: nobody
Labels: None
Priority: 5
Updated: 2021-04-11
Created: 2021-04-11
Creator: rc0r
Private: No

Description

Function `ezxml_internal_dtd()` performs incorrect memory handling while parsing crafted XML files which leads to a NULL pointer dereference during `strcmp()`.

MITRE assigned **CVE-2021-30485** for this issue.

Debugging Output

```
$ gdb ~/tmp/ezxml/ezxml_test CVE-2021-30485-nullptr-000.sample
>>> r
Program received signal SIGSEGV, Segmentation fault.
0x00007ffff7f0b9fe in __strcmp_avx2 () from /usr/lib/libc.so.6

Assembly
>0x00007ffff7f0b9fe  c5 fe 6f 0f  ? vmovdqu ymm1,YMMWORD PTR [rdi]
 0x00007ffff7f0ba02  c5 f5 74 06  ? vpcmpeqb ymm0,ymm1,YMMWORD PTR [rsi]
 0x00007ffff7f0ba06  c5 fd da c1  ? vpminub ymm0,ymm0,ymm1
 0x00007ffff7f0ba0a  c5 fd 74 c7  ? vpcmpeqb ymm0,ymm0,ymm7
 0x00007ffff7f0ba0e  c5 fd d7 c8  ? vpmovmskb ecx,ymm0
 0x00007ffff7f0ba12  85 c9        ? test   ecx,ecx
 0x00007ffff7f0ba14  74 7a        ? je     0x7ffff7f0ba90 <__strcmp_avx2+176>
 0x00007ffff7f0ba16  f3 0f bc d1  ? tzcnt  edx,ecx
 0x00007ffff7f0ba1a  0f b6 04 17  ? movzx  eax,BYTE PTR [rdi+rdx*1]
 0x00007ffff7f0ba1e  0f b6 14 16  ? movzx  edx,BYTE PTR [rsi+rdx*1]

>>> i r
rax            0x13                19
rbx            0x55555555b2c0      93824992260800
rcx            0x0                 0
rdx            0x0                 0
rsi            0x7ffff7ffa013      140737354113043
rdi            0x0                 0
rbp            0x7fffffffd7d0      0x7fffffffd7d0
rsp            0x7fffffffd6e8      0x7fffffffd6e8
r8             0x55555555c1b0      93824992264624
r9             0x7ffff7f70a60      140737353550432
r10            0xfffffffffffffb8e  -1138
r11            0x7ffff7f0b9e0      140737353136608
r12            0x555555555250      93824992236112
r13            0x0                 0
r14            0x0                 0
r15            0x0                 0
rip            0x7ffff7f0b9fe      0x7ffff7f0b9fe <__strcmp_avx2+30>
eflags         0x10287             [ CF PF SF IF RF ]
cs             0x33                51
ss             0x2b                43
ds             0x0                 0
es             0x0                 0
fs             0x0                 0
gs             0x0                 0

>>> bt
#0  0x00007ffff7f0b9fe in __strcmp_avx2 () from /usr/lib/libc.so.6
#1  0x00005555555567e3 in ezxml_internal_dtd (root=root@entry=0x55555555d2a0, s=0x7ffff7ffa
#2  0x00005555555588d1 in ezxml_parse_str (s=<optimized out>, s@entry=0x7ffff7ffa000 "<!DOC
#3  0x0000555555558b59 in ezxml_parse_fd (fd=fd@entry=3) at ezxml.c:641
#4  0x0000555555558bfb in ezxml_parse_file (file=<optimized out>) at ezxml.c:659
#5  0x000055555555526a in main (argc=<optimized out>, argv=<optimized out>) at ezxml.c:1008

>>> up
#1  0x00005555555567e3 in ezxml_internal_dtd (root=root@entry=0x55555555d2a0, s=0x7ffff7ffa
362                 for (i = 0; root->attr[i] && strcmp(n, root->attr[i][0]); i++);
```

Reproduction

```
$ cd ~/tmp/ezxml
$ gcc -Wall -O2 -DEZXML_TEST -g -ggdb -o ezxml_test ezxml.c
$ gdb ~/tmp/ezxml/ezxml_test CVE-2021-30485-nullptr-000.sample
```

Patch

The following patch adds a check for the NULL pointer condition.

```
diff --git a/ezxml.c b/ezxml-fixed.c
index 82b11fb..b904d4e 100644
--- a/ezxml.c
+++ b/ezxml-fixed.c
@@ -359,7 +359,7 @@ short ezxml_internal_dtd(ezxml_root_t root, char *s, size_t len)
             if (! *t) { ezxml_err(root, t, "unclosed <!ATTLIST"); break; }
             if (*(s = t + strcspn(t, EZXML_WS ">")) == '>') continue;
             else *s = '\0'; // null terminate tag name
-            for (i = 0; root->attr[i] && strcmp(n, root->attr[i][0]); i++);
+            for (i = 0; n && root->attr[i] && strcmp(n, root->attr[i][0]); i++);

             while (*(n = ++s + strspn(s, EZXML_WS)) && *n != '>') {
                 if (*(s = n + strcspn(n, EZXML_WS))) *s = '\0'; // attr name
```

Files

- CVE-2021-30485-nullptr-000.sample (Crash sample)
- CVE-2021-30485-nullptr-000.patch (Patch adding NULL ptr check)

2 Attachments

CVE-2021-30485-nullptr-000.patch

CVE-2021-30485-nullptr-000.sample

Discussion

Log in to post a comment.