bug-cflow

[Top][All Lists]
Search Advanced

[Date Prev][Date Next][Thread Prev][Thread Next][Date Index][Thread Index]

cflow 1.6 "void call(char *name, int line)" function Use-after-Free vuln

From: address@hidden
Subject: cflow 1.6 "void call(char *name, int line)" function Use-after-Free vulnerability
Date: Thu, 9 Jul 2020 10:33:22 +0800

Hello,
I have found an Use-after-Free vulnerability in cflow 1.6 "void call(char *name, int line)" function.
Description:
There is a Use-after-Free bug in void call(char *name, int line) function at src/parser.c: line 1284.
An attacker can exploit this bug to cause a Denial of Service (DoS) by submitting a malicious PoC source file.
This bug is caused by the using of pointer variable caller->callee, this variable is freed in parser.c line 298 type = get_token(). The using of caller->callee triggered a Use-after-Free bug.

We used AddressSanitizer instrumented in cflow and triggered this bug, the output of asan as follow:

```
ASAN_OPTIONS=detect_leaks=0 ./cflow ./out_dir/PoC_cflow_uaf_parser_line1284 --tree --format=posix --all /dev/null
./cflow:libavutil/intreadwrite.h:50115054: buf redefined
./cflow:libavutil/intreadwrite.h:50115052: this is the place of previous definition
./cflow:libavutil/intreadwrite.h:50115055: buf redefined
./cflow:libavutil/intreadwrite.h:50115054: this is the place of previous definition
./cflow:libavutil/intreadwrite.h:50115057: buf redefined
./cflow:libavutil/intreadwrite.h:50115055: this is the place of previous definition
./cflow:libavutil/intreadwrite.h:50115059: buf redefined
./cflow:libavutil/intreadwrite.h:50115057: this is the place of previous definition
./cflow:libavutil/intreadwrite.h:50115194: unterminated string?
./cflow:libavutil/intreadwrite.h:50115195: unterminated string?
./cflow:libavutil/intreadwrite.h:50115196: unterminated string?
./cflow:libavutil/intreadwrite.h:50115197: unterminated string?
./cflow:libavutil/intreadwrite.h:50115198: unterminated string?
./cflow:libavutil/intreadwrite.h:50115199: unterminated string?
./cflow:libavutil/intreadwrite.h:50115200: unterminated string?
./cflow:libavutil/intreadwrite.h:50115201: unterminated string?
./cflow:libavutil/intreadwrite.h:50115202: unterminated string?
./cflow:libavutil/intreadwrite.h:50115203: unterminated string?
./cflow:libavutil/intreadwrite.h:50115204: unterminated string?
./cflow:libavutil/intreadwrite.h:50115205: unterminated string?
./cflow:libavutil/intreadwrite.h:50115206: unterminated string?
./cflow:libavutil/intreadwrite.h:50115207: unterminated string?
./cflow:libavutil/intreadwrite.h:50115208: unterminated string?
./cflow:libavutil/intreadwrite.h:50115209: unterminated string?
./cflow:libavutil/intreadwrite.h:50115210: unterminated string?
./cflow:libavutil/intreadwrite.h:50115211: unterminated string?
./cflow:libavutil/intreadwrite.h:50115212: unterminated string?
./cflow:libavutil/intreadwrite.h:50115213: unterminated string?
./cflow:libavutil/intreadwrite.h:50115214: unterminated string?
./cflow:libavutil/intreadwrite.h:50115215: unterminated string?
./cflow:libavutil/intreadwrite.h:50115216: unterminated string?
./cflow:libavutil/intreadwrite.h:50115217: unterminated string?
./cflow:libavutil/intreadwrite.h:50115218: unterminated string?
./cflow:libavutil/intreadwrite.h:50115219: unterminated string?
./cflow:libavutil/intreadwrite.h:50115220: unterminated string?
./cflow:libavutil/intreadwrite.h:50115221: unterminated string?
./cflow:libavutil/intreadwrite.h:50115222: unterminated string?
./cflow:libavutil/intreadwrite.h:50115223: unterminated string?
./cflow:libavutil/intreadwrite.h:50115224: unterminated string?
./cflow:libavutil/intreadwrite.h:50115225: unterminated string?
./cflow:libavutil/intreadwrite.h:50115226: unterminated string?
./cflow:libavutil/intreadwrite.h:50115227: unterminated string?
./cflow:libavutil/intreadwrite.h:50115228: unterminated string?
./cflow:libavutil/intreadwrite.h:50115229: unterminated string?
./cflow:libavutil/intreadwrite.h:50115230: unterminated string?
./cflow:libavutil/intreadwrite.h:50115231: unterminated string?
./cflow:libavutil/intreadwrite.h:50115232: unterminated string?
./cflow:libavutil/intreadwrite.h:50115233: unterminated string?
./cflow:libavutil/intreadwrite.h:50115234: unterminated string?
./cflow:libavutil/intreadwrite.h:50115235: unterminated string?
./cflow:libavutil/intreadwrite.h:50115236: unterminated string?
./cflow:libavutil/intreadwrite.h:50115237: unterminated string?
./cflow:libavutil/intreadwrite.h:50115238: unterminated string?
./cflow:libavutil/intreadwrite.h:50115239: unterminated string?
./cflow:libavutil/intreadwrite.h:50115240: unterminated string?
./cflow:libavutil/intreadwrite.h:50115241: unterminated string?
./cflow:libavutil/intreadwrite.h:50115242: unterminated string?
./cflow:libavutil/intreadwrite.h:50115243: unterminated string?
./cflow:libavutil/intreadwrite.h:50115244: unterminated string?
./cflow:libavutil/intreadwrite.h:50115245: unterminated string?
```

```
./cflow:libavutil/intreadwrite.h:50115246: unterminated string?
./cflow:libavutil/intreadwrite.h:50115247: unterminated string?
./cflow:libavutil/intreadwrite.h:50115248: unterminated string?
./cflow:libavutil/intreadwrite.h:50115249: unterminated string?
./cflow:libavutil/intreadwrite.h:50115250: unterminated string?
./cflow:libavutil/intreadwrite.h:50115251: unterminated string?
./cflow:libavutil/intreadwrite.h:50115252: unterminated string?
./cflow:libavutil/intreadwrite.h:50115253: unterminated string?
./cflow:libavutil/intreadwrite.h:50115254: unterminated string?
libavutil/intreadwrite.h:50115254: unexpected end of file in struct
=================================================================
==57157==ERROR: AddressSanitizer: heap-use-after-free on address 0x60e000003630 at pc 0x00000053f773 bp 0x7ffd4f2a1c50 sp 0x7ffd4f2a1c48
READ of size 8 at 0x60e000003630 thread T0
    #0 0x53f772 in call /root/experiment/cflow-1.6/src/parser.c:1284:34
    #1 0x53f772 in _expression_ /root/experiment/cflow-1.6/src/parser.c:618:7
    #2 0x537ced in func_body /root/experiment/cflow-1.6/src/parser.c:1051:9
    #3 0x537ced in parse_function_declaration /root/experiment/cflow-1.6/src/parser.c:690:9
    #4 0x53634e in parse_declaration /root/experiment/cflow-1.6/src/parser.c:578:4
    #5 0x53407c in yyparse /root/experiment/cflow-1.6/src/parser.c:528:9
    #6 0x51695e in main /root/experiment/cflow-1.6/src/main.c:812:7
    #7 0x7f86f4490b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310
    #8 0x41c109 in _start (/root/experiment/cflow-1.6/src/cflow+0x41c109)

0x60e000003630 is located 144 bytes inside of 152-byte region [0x60e0000035a0,0x60e000003638)
freed by thread T0 here:
    #0 0x4a9370 in free /root/Downloads/llvm-build/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cpp:123
    #1 0x5157b4 in linked_list_destroy /root/experiment/cflow-1.6/src/linked-list.c:87:7
    #2 0x4f161e in yywrap /root/experiment/cflow-1.6/src/c.l:366:6
    #3 0x4f161e in yylex /root/experiment/cflow-1.6/src/c.c:1653:10
    #4 0x504edd in get_token /root/experiment/cflow-1.6/src/c.l:380:17
    #5 0x544c11 in nexttoken /root/experiment/cflow-1.6/src/parser.c:298:11
    #6 0x544c11 in skip_balanced /root/experiment/cflow-1.6/src/parser.c:483:13
    #7 0x544c11 in skip_struct /root/experiment/cflow-1.6/src/parser.c:836:8
    #8 0x538f91 in parse_variable_declaration /root/experiment/cflow-1.6/src/parser.c:732:4
    #9 0x537cc1 in func_body /root/experiment/cflow-1.6/src/parser.c:1061:9
    #10 0x537cc1 in parse_function_declaration /root/experiment/cflow-1.6/src/parser.c:690:9
    #11 0x53634e in parse_declaration /root/experiment/cflow-1.6/src/parser.c:578:4
    #12 0x53407c in yyparse /root/experiment/cflow-1.6/src/parser.c:528:9
    #13 0x51695e in main /root/experiment/cflow-1.6/src/main.c:812:7
    #14 0x7f86f4490b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310

previously allocated by thread T0 here:
    #0 0x4a9690 in malloc /root/Downloads/llvm-build/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x5a01ab in xmalloc /root/experiment/cflow-1.6/gnu/xmalloc.c:43:13
    #2 0x556567 in install /root/experiment/cflow-1.6/src/symbol.c:92:12
    #3 0x556567 in install_ident /root/experiment/cflow-1.6/src/symbol.c:156:11
    #4 0x5427fd in get_symbol /root/experiment/cflow-1.6/src/parser.c:1249:13
    #5 0x5427fd in declare /root/experiment/cflow-1.6/src/parser.c:1178:11
    #6 0x5427fd in parse_dcl /root/experiment/cflow-1.6/src/parser.c:879:4
    #7 0x536969 in parse_knr_dcl /root/experiment/cflow-1.6/src/parser.c:824:6
    #8 0x536969 in parse_function_declaration /root/experiment/cflow-1.6/src/parser.c:663:6
    #9 0x53634e in parse_declaration /root/experiment/cflow-1.6/src/parser.c:578:4
    #10 0x53407c in yyparse /root/experiment/cflow-1.6/src/parser.c:528:9
    #11 0x51695e in main /root/experiment/cflow-1.6/src/main.c:812:7
    #12 0x7f86f4490b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310

SUMMARY: AddressSanitizer: heap-use-after-free /root/experiment/cflow-1.6/src/parser.c:1284:34 in call
Shadow bytes around the buggy address:
  0x0c1c7fff8670: 00 00 00 fa fa fa fa fa fa fa fa fa 00 00 00 00
  0x0c1c7fff8680: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa
  0x0c1c7fff8690: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c1c7fff86a0: 00 00 00 00 00 00 00 00 00 00 00 00 fa fa fa fa
  0x0c1c7fff86b0: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c1c7fff86c0: fd fd fd fd fd fd[fd]fa fa fa fa fa fa fa fa fa
  0x0c1c7fff86d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c1c7fff86e0: 00 00 00 fa fa fa fa fa fa fa fa fa 00 00 00 00
  0x0c1c7fff86f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa
  0x0c1c7fff8700: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c1c7fff8710: fd fd fd fd fd fd fd fd fd fd fd 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
==57157==ABORTING
```

We used GDB to debug this bug, the GDB outputs:

```
gdb-peda$ set args ./out_dir/PoC_cflow_uaf_parser_line1284 --tree --format=posix --all /dev/null
gdb-peda$ b * 0x53f772
Breakpoint 1 at 0x53f772: file parser.c, line 1284.
gdb-peda$ r
Starting program: /root/experiment/cflow-1.6/src/cflow ./out_dir/PoC_cflow_uaf_parser_line1284 --tree --format=posix --all /dev/null
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115054: buf redefined
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115052: this is the place of previous definition
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115055: buf redefined
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115054: this is the place of previous definition
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115057: buf redefined
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115055: this is the place of previous definition
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115059: buf redefined
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115057: this is the place of previous definition
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115194: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115195: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115196: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115197: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115198: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115199: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115200: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115201: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115202: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115203: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115204: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115205: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115206: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115207: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115208: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115209: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115210: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115211: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115212: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115213: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115214: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115215: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115238: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115239: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115240: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115241: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115242: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115243: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115244: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115245: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115246: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115247: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115248: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115249: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115250: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115251: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115252: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115253: unterminated string?
/root/experiment/cflow-1.6/src/cflow:libavutil/intreadwrite.h:50115254: unterminated string?
libavutil/intreadwrite.h:50115254: unexpected end of file in struct
Program received signal SIGSEGV, Segmentation fault.

[----------------------------------registers-----------------------------------]
RAX: 0xc1c000006c6 --> 0x0
RBX: 0x0
RCX: 0x82b018 --> 0x10db3e0 --> 0x10100fbfb00 --> 0x0
RDX: 0x0
RSI: 0x6455738 --> 0x0
RDI: 0x60e000003630 --> 0x0
RBP: 0x7fffffffdfb0 --> 0x7fffffffe110 --> 0x7fffffffe1b0 --> 0x7fffffffe350 --> 0x7fffffffe480 --> 0x5ce1a0 (<__libc_csu_init>:     push   r15)
RSP: 0x7fffffffdf18 --> 0x53f773 (<_expression_+11939>:        mov    edi,0xa0e7618)
RIP: 0xffffffffcd4b74a0
R8 : 0x40 ('@')
R9 : 0x3
R10: 0x7ffff7fd0000 --> 0x7ffff7fe7000 --> 0x81a758 --> 0x4bacd0 (<__sanitizer::ThreadContextBase::OnDead()>:        repz ret)
```

```
R11: 0x7ffff6e24b97 (<__libc_start_main+231>:	mov    edi,eax)
R12: 0x141cec4 --> 0x0
R13: 0x60e000004100 --> 0x602000001dd0 (0x000060e000004100)
R14: 0xc1c0000082e --> 0x0
R15: 0x60e000004188 --> 0x6030000034f0 --> 0x0
EFLAGS: 0x10282 (carry parity adjust zero SIGN trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
Invalid $PC address: 0xffffffffcd4b74a0
[------------------------------------stack-------------------------------------]
0000| 0x7fffffffdf18 --> 0x53f773 (<_expression_+11939>:	mov    edi,0xa0e7618)
0008| 0x7fffffffdf20 --> 0x141cebf --> 0x0
0016| 0x7fffffffdf28 --> 0x141cec0 --> 0x0
0024| 0x7fffffffdf30 --> 0xffffffffbfd --> 0x0
0032| 0x7fffffffdf38 --> 0x141ce93 --> 0x0
0040| 0x7fffffffdf40 --> 0x2fcb26effffdfe0
0048| 0x7fffffffdf48 --> 0x141ce91 --> 0x0
0056| 0x7fffffffdf50 --> 0x141cebe --> 0x0
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
0xffffffffcd4b74a0 in ?? ()
```

We could clearly observe the Use-after-Free in call() function at 0x53f772 and ensure this bug can finish a DoS attack.
You can reproduce this UaF vulnerability by the follow step:

```
./cflow PoC_cflow_uaf_parser_line1284 --tree --format=posix --all /dev/null
```

If you want to use asan to reproduce this vulnerability, you should use ASAN option as follows:

```
ASAN_OPTIONS=detect_leaks=0 ./cflow PoC_cflow_uaf_parser_line1284 --tree --format=posix --all /dev/null
```

You can download the PoC at:
https://github.com/yangjiageng/PoC/blob/master/PoC_cflow_uaf_parser_line1284

If you have any question, please let me know.

yangmew@outlook.com

PoC_cflow_uaf_parser_line1284
Description: Binary data

reply via email to
address@hidden

[Prev in Thread] **Current Thread** [Next in Thread]

- **cflow 1.6 "void call(char *name, int line)" function Use-after-Free vulnerability**, *address@hidden* <=

- Index(es):
  - **Date**
  - **Thread**