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

An illegal memory access in ncurses, tic

From: 郑晗
Subject: An illegal memory access in ncurses, tic
Date: Sat, 16 Apr 2022 21:19:48 +0800 (GMT+08:00)

Dear developers,

I'm a security researcher and is now trying to test my new fuzzer. I've just found an illegal memory access in the latest commit of ncurse, tic. Here are the informations:

(1) environment
Ubuntu 20.04.3 LTS
gcc 9.3.0
ncurse latest commit 74b10d4a30eec8feb66a4b94a72da65be0048447, tag v6_3_20220409

(2) step to reproduce:

```
export CFLAGS="-fsanitze=address -g"
export CXXFLAGS="-fsanitize=address -g"
./configure &amp;&amp; make -j$(nproc)
./prog/tic -o /dev/null $POC
```

(3) ASAN Report

```
"poc", line 2, col 812, terminal 'pse': slashes aren't allowed in names or
aliases
"poc", line 3, col 10, terminal 'pse': Illegal character - '~H'
"poc", line 3, col 10, terminal 'pse': unknown capability 'a'
"poc", line 3, col 11, terminal 'pse': Illegal character (expected alphanumeric
or @%&amp;*!#) - '='
"poc", line 4, col 9, terminal 'pse': Illegal character (expected alphanumeric
or @%&amp;*!#) - '&gt;'
"poc", line 4, col 12, terminal 'pse': Illegal character - '^J'
"poc", line 4, col 12, terminal 'pse': unknown capability 'H'
"poc", line 6, col 15, terminal 'pse': unknown capability '@E'
"poc", line 8, col 9, terminal 'pse': Illegal character (expected alphanumeric
or @%&amp;*!#) - 'M-:'
"poc", line 9, col 6, terminal 'pse': unknown capability 'rlrm'
"poc", line 9, col 12, terminal 'pse': Missing separator after `ptlr', have r
"poc", line 9, col 14, terminal 'pse': Illegal character - '~@'
"poc", line 9, col 14, terminal 'pse': unknown capability 'l'
"poc", line 9, col 16, terminal 'pse': Illegal character (expected alphanumeric
or @%&amp;*!#) - ':'
"poc", line 9, col 23, terminal 'pse': Illegal character (expected alphanumeric
or @%&amp;*!#) - '~@'
"poc", line 1, col 2, terminal 'pse': cannot link alias erm,�cutl,r/term,ial.
"poc", line 1, col 2, terminal 'pse': alias ProT multiply defined.
"poc", line 13, col 9, terminal 'm': Legacy termcap allows only a trailing tc=
clause
"poc", line 13, col 13, terminal 'm': Illegal character - '^'
```

```
"poc", line 13, col 13, terminal 'm': wrong type used for string capability
'@8Y'
"poc", line 13, col 15, terminal 'm': unknown capability 'M'
"poc", line 13, col 17, terminal 'm': unknown capability 'I'
"poc", line 13, col 19, terminal 'm': Illegal character - '^J'
"poc", line 13, col 19, terminal 'm': unknown capability 'n'
"poc", line 14, col 23, terminal 'm': Missing separator
"poc", line 15, col 19, terminal 'm': Illegal character - '%'
"poc", line 15, col 19, terminal 'm': unknown capability 'k'
"poc", line 15, col 21, terminal 'm': Illegal character - '%'
"poc", line 15, col 21, terminal 'm': unknown capability 'r'
"poc", line 15, col 22, terminal 'm': Illegal character (expected alphanumeric
or @%&amp;*!#) - '^?'
"poc", line 17, col 9, terminal 'm': Illegal character (expected alphanumeric
or @%&amp;*!#) - '&gt;'
"poc", line 19, col 13, terminal 'm': Illegal character - '^'
"poc", line 19, col 13, terminal 'm': wrong type used for string capability
'@8Y'
"poc", line 19, col 15, terminal 'm': unknown capability 'M'
"poc", line 19, col 17, terminal 'm': unknown capability 'j'
"poc", line 19, col 19, terminal 'm': Illegal character - '^J'
"poc", line 19, col 19, terminal 'm': unknown capability 'p'
"poc", line 21, col 15, terminal 'm': unknown capability 'Cdc'
"poc", line 22, col 9, terminal 'm': Illegal character (expected alphanumeric
or @%&amp;*!#) - '['
"poc", line 22, col 18, terminal 'm': Illegal character - '^J'
"poc", line 22, col 18, terminal 'm': wrong type used for boolean capability
'in'
"poc", line 24, col 12, terminal 'm': Illegal character - '^?'
"poc", line 24, col 12, terminal 'm': wrong type used for string capability 'r1'
"poc", line 24, col 13, terminal 'm': Illegal character (expected alphanumeric
or @%&amp;*!#) - '^'
"poc", line 26, col 23, terminal 'm': Illegal character (expected alphanumeric
or @%&amp;*!#) - '^'
"poc", line 27, col 9, terminal 'm': Illegal character (expected alphanumeric
or @%&amp;*!#) - '/'
"poc", line 31, col 0, terminal 'm': Missing separator
"poc", line 31, col 1, terminal 'm': Illegal character (expected alphanumeric
or @%&amp;*!#) - '='
AddressSanitizer:DEADLYSIGNAL
=================================================================
==3827912==ERROR: AddressSanitizer: SEGV on unknown address 0x615fffffdc51 (pc
0x557e8341653e bp 0x7ffda95d3a70 sp 0x7ffda95d3a40 T0)
==3827912==The signal is caused by a READ memory access.
    #0 0x557e8341653d in convert_strings ../ncurses/./tinfo/read_entry.c:164
    #1 0x557e834178a3 in _nc_read_termtype ../ncurses/./tinfo/read_entry.c:370
    #2 0x557e83418cc0 in _nc_read_file_entry ../ncurses/./tinfo/read_entry.c:566
    #3 0x557e834199e4 in _nc_read_tic_entry ../ncurses/./tinfo/read_entry.c:820
    #4 0x557e83419c8f in _nc_read_entry ../ncurses/./tinfo/read_entry.c:864
    #5 0x557e83424781 in _nc_resolve_uses2 ../ncurses/./tinfo/comp_parse.c:473
    #6 0x557e833df5c1 in main ../progs/tic.c:972
    #7 0x7f05db7a20b2 in __libc_start_main
(/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #8 0x557e833dbe0d in _start
(/home/hzheng/real-validate/ncurses-snapshots/progs/tic+0x37e0d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV ../ncurses/./tinfo/read_entry.c:164 in
convert_strings
==3827912==ABORTING
```

(4) POC
as shown in the attachment

(5) Credit

```
NCNIPC of China
```

[poc0.zip]
Description: Zip compressed data

---

reply via email to

郑晗

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

- **An illegal memory access in ncurses, tic**, *郑晗* <=
  - **Re: An illegal memory access in ncurses, tic**, *Thomas Dickey*, `2022/04/16`
    - **Re: An illegal memory access in ncurses, tic**, *Thomas Dickey*, `2022/04/16`
      - **Re: An illegal memory access in ncurses, tic**, *郑晗*, `2022/04/17`

- Prev by Date: **Re: Issue with unget_wch_sp and -D_FORTIFY_SOURCE**
- Next by Date: **Re: An illegal memory access in ncurses, tic**
- Previous by thread: **ANN: ncurses-6.3-20220409**
- Next by thread: **Re: An illegal memory access in ncurses, tic**
- Index(es):
  - **Date**
  - **Thread**