


 **owntone / owntone-server** Public[Code](#) [Issues](#) 106 [Pull requests](#) 7 [Actions](#) [Wiki](#) [Security and quality](#)[New issue](#)

Stack overflow #1873

✓ Closed wenwenyuyu opened on Mar 7, 2025 ⋮


Hello, I conducted fuzzing tests on owntone-server and discovered a stack buffer overflow vulnerability.

This is my test case.

[poc.txt](#)


version: [2ca10d9](#)

platform: ubuntu20.04


 wenwenyuyu on Mar 7, 2025 Author ⋮

AddressSanitizer result:

[result.txt](#)

 ejurgensen on Mar 7, 2025 Member ⋮

Thanks for this, I think that issue might still be present, so I will get it fixed. I'm a bit puzzled as to why you are testing with a version of OwnTone (then forked-daapd) that is 5 years old?

 wenwenyuyu on Mar 7, 2025 Author ⋮

I tested on Profuzzbench, and since the version there is five years old, I didn't make any changes :)

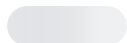


wenwenyuyu closed this as completed on Mar 15, 2025



ejurgensen added a commit that references this issue on Mar 15, 2025

[parsers] Fix possible stack overflow from recursion



13a8f71

[Sign up for free](#) to join this conversation on **GitHub**. Already have an account? [Sign in to comment](#)

Metadata

Assignees

No one assigned

Labels

No labels

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with agent mode ▼

No branches or pull requests

Participants



