COMMUNITY CONTENT

Home › Submit › 780560

Submit #780560: nothings stb (stb_vorbis.c) ≤ 1.22 Free of Pointer not at Start of Buffer

Title	nothings stb (stb_vorbis.c) ≤ 1.22 Free of Pointer not at Start of Buffer
Description	An invalid free vulnerability exists in `setup_free()` in stb_vorbis.c v1.22 and earlier. When processing a crafted Ogg Vorbis file, the `vorbis_deinit()` function at line 4214 calls `setup_free()` at line 966 to free internal decoder structures. Due to corrupted internal state from malformed Vorbis setup headers, `setup_free()` attempts to free an invalid pointer, causing a crash in the memory allocator. This is triggered via `stb_vorbis_open_memory()` or `stb_vorbis_decode_memory()` when the decoder encounters an error during setup and attempts cleanup. The crash occurs inside the allocator's `Deallocate()` function due to an invalid pointer being passed to `free()`. ASAN output: ``` ERROR: AddressSanitizer: SEGV on unknown address READ memory access in __asan::Allocator::Deallocate #1 free #2 setup_free stb_vorbis.c:966 #3 vorbis_deinit stb_vorbis.c:4214 #4 stb_vorbis_open_memory stb_vorbis.c:5122 #5 stb_vorbis_decode_memory stb_vorbis.c:5390 ```
Source	https://gist.github.com/d0razi/cc7f70bba08c1a455d9933e97b8b57c1
User	d0razi (UID 96474)
Submission	03/16/2026 01:15 AM (17 days ago)
Moderation	04/01/2026 02:40 PM (17 days later)
Status	Published
VulDB entry	[Nothings stb up to 1.22 stb_vorbis.c setup_free allocation of resources]
Points	20

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling