xiph / speex Public

<> Code ⊙ Issues 4 Pull requests 3 Actions Projects Wiki ···

New issue

Jump to bottom

speexenc encode wav file dos vulnerability #13

Closed **Aurorainfinity** opened this issue on Jul 13, 2020 · 2 comments

Aurorainfinity commented on Jul 13, 2020

when speexenc encode wav file , deal with channels 0 will generate a Division by zero error which will cause the software crash
sample.tar.gz
usage :
speexenc sample -

vulnerability function:
static int read_samples(FILE *fin,int frame_size, int bits, int channels, int lsb, short * input, char *buff, spx_int32_t *size)*
{
*unsigned char in[MAX_FRAME_BYTES*2];
int i;
short *s;
int nb_read;
size_t to_read;

if (size && *size<=0)
{
return 0;
}

to_read = bits/8*channels*frame_size;

tmatth commented on Jul 14, 2020 Member

@Aurorainfinity thanks, there's a fix waiting for review here if you want to test it out:
https://gitlab.xiph.org/xiph/speex/-/merge_requests/1

FYI: We only use github as a mirror, that's why the MR is over on our gitlab instance.

tmatth closed this as completed in `870ff84` on Sep 22, 2020

tmatth commented on Feb 11 • edited Member

Just to clarify, the code in question is **not part of the libspeex library**, it's only part of the `speexenc` example program.

jlaine mentioned this issue on Mar 25

Vulnerability PyAV-Org/PyAV#921

Closed

6 tasks

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants