CVE-2017-8373

描述：The mad\_layer\_III function in layer3.c in Underbit MAD libmad 0.15.1b allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted audio file.

软件：Underbit MAD libmad 0.15.1b

源码：libmad-0.15.1b/layer3.c

出现位置： 2627-2640行

关键源码：

else {

mad\_bit\_init(&ptr,

\*stream->main\_data + stream->md\_len - si.main\_data\_begin);

if (md\_len > si.main\_data\_begin) {

assert(stream->md\_len + md\_len -

si.main\_data\_begin <= MAD\_BUFFER\_MDLEN);

memcpy(\*stream->main\_data + stream->md\_len,

mad\_bit\_nextbyte(&stream->ptr),

frame\_used = md\_len - si.main\_data\_begin);

stream->md\_len += frame\_used;

}