CVE-2017-8374

描述：The mad\_bit\_skip function in bit.c in Underbit MAD libmad 0.15.1b allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted audio file.

软件：libmad 0.15.1b

源码：bit.c

出现位置： 119-131行

关键源码：

void mad\_bit\_skip(struct mad\_bitptr \*bitptr, unsigned int len)

{

bitptr->byte += len / CHAR\_BIT;

bitptr->left -= len % CHAR\_BIT;

if (bitptr->left > CHAR\_BIT) {

bitptr->byte++;

bitptr->left += CHAR\_BIT;

}

if (bitptr->left < CHAR\_BIT)

bitptr->cache = \*bitptr->byte; //buffer overflow

}