CVE-2017-7586

描述：In libsndfile before 1.0.28, an error in the "header\_read()" function (common.c) when handling ID3 tags can be exploited to cause a stack-based buffer overflow via a specially crafted FLAC file.

软件：libsndfile

源码：src/common.c

出现位置： 823-851行

关键源码：

static int

header\_read (SF\_PRIVATE \*psf, void \*ptr, int bytes)

{ int count = 0 ;

if (psf->headindex >= SIGNED\_SIZEOF (psf->header))

return psf\_fread (ptr, 1, bytes, psf) ;

if (psf->headindex + bytes > SIGNED\_SIZEOF (psf->header))

{ int most ;

most = SIGNED\_SIZEOF (psf->header) - psf->headend ;

psf\_fread (psf->header + psf->headend, 1, most, psf) ;

memcpy (ptr, psf->header + psf->headend, most) ;

psf->headend = psf->headindex += most ;

psf\_fread ((char \*) ptr + most, bytes - most, 1, psf) ;

return bytes ;

} ;

if (psf->headindex + bytes > psf->headend)

{ count = psf\_fread (psf->header + psf->headend, 1, bytes - (psf->headend - psf->headindex), psf) ;

if (count != bytes - (int) (psf->headend - psf->headindex))

{ psf\_log\_printf (psf, "Error : psf\_fread returned short count.\n") ;

return count ;

} ;

psf->headend += count ;

} ;

memcpy (ptr, psf->header + psf->headindex, bytes) ;

psf->headindex += bytes ;