CVE-2017-5975

描述：Heap-based buffer overflow in the \_\_zzip\_get64 function in fetch.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (crash) via a crafted ZIP file.

软件：zziplib 0.13.62

源码：/zzip/fetch.c

出现位置： 54-68行

关键源码：

\_\_zzip\_get64(unsigned char \*s)

{

#ifdef \_\_GNUC\_\_

/\* \*INDENT-OFF\* \*/

register uint64\_t v

= s[7]; v <<= 8;

v |= s[6]; v <<= 8;

v |= s[5]; v <<= 8;

v |= s[4]; v <<= 8;

v |= s[3]; v <<= 8;

v |= s[2]; v <<= 8;

v |= s[1]; v <<= 8;

v |= s[0]; return v;

/\* \*INDENT-ON\* \*/

#else