CVE-2017-5976

描述：Heap-based buffer overflow in the zzip\_mem\_entry\_extra\_block function in memdisk.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/memdisk.c

出现位置： 243-264行

关键源码：

while (1)

{

ZZIP\_EXTRA\_BLOCK \*ext = entry->zz\_ext[i];

if (ext)

{

while (\*(short \*) (ext->z\_datatype))

{

if (datatype == zzip\_extra\_block\_get\_datatype(ext))

{

return ext;

}

\_\_\_ char \*e = (char \*) ext;

e += zzip\_extra\_block\_headerlength;

e += zzip\_extra\_block\_get\_datasize(ext);

ext = (void \*) e;

\_\_\_\_;

}

}

if (! i)

return 0;

i--;

}