CVE-2017-8364

描述：The read\_buf function in stream.c in rzip 2.1 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 archive.

软件：rzip 2.1

源码：src/stream.c

出现位置： 150-163行

关键源码：

static int read\_buf(int f, uchar \*p, int len)

{

int ret;

ret = read(f, p, len); //heap-based buffer overflow

if (ret == -1) {

err\_msg("Read of length %d failed - %s\n", len, strerror(errno));

return -1;

}

if (ret != len) {

err\_msg("Partial read!? asked for %d bytes but got %d\n", len, ret);

return -1;

}

return 0;

}