CVE-2016-10196

描述：Stack-based buffer overflow in the evutil\_parse\_sockaddr\_port function in evutil.c in libevent before 2.1.6-beta allows attackers to cause a denial of service (segmentation fault) via vectors involving a long string in brackets in the ip\_as\_string argument.

软件：libevent

源码：evutil.c

出现位置：2060-2071行

关键源码：

if (\*ip\_as\_string == '[') {

int len;

if (!(cp = strchr(ip\_as\_string, ']'))) {

return -1;

}

len = (int) ( cp-(ip\_as\_string + 1) );

if (len > (int)sizeof(buf)-1) {

return -1;

}

memcpy(buf, ip\_as\_string+1, len);

buf[len] = '\0';

addr\_part = buf;