CVE-2017-6191

描述：Buffer overflow in APNGDis 2.8 and below allows a remote attacker to execute arbitrary code via a crafted filename.

软件：APNGDis 2.8

源码： apngdis.cpp

出现位置：474 行

关键源码：

if (argc > 1)

szInput = argv[1];

else

{

printf("Usage: apngdis anim.png [name]\n");

return 1;

}

strcpy(szPath, szInput);