CVE-2017-7187

描述：The sg\_ioctl function in drivers/scsi/sg.c in the Linux kernel through 4.10.4 allows local users to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a large command size in an SG\_NEXT\_CMD\_LEN ioctl call, leading to out-of-bounds write access in the sg\_write function.

软件：Linux kernel

源码：drivers/scsi/sg.c

出现位置：996-1002行

关键源码：

@@ -996,6 +996,8 @@ sg\_ioctl(struct file \*filp, unsigned int cmd\_in, unsigned long arg)

result = get\_user(val, ip);

if (result)

return result;

+ if (val > SG\_MAX\_CDB\_SIZE)

+ return -ENOMEM;

sfp->next\_cmd\_len = (val > 0) ? val : 0;

return 0;

case SG\_GET\_VERSION\_NUM: