CVE-2015-8613

描述：Stack-based buffer overflow in the megasas\_ctrl\_get\_info function in QEMU, when built with SCSI MegaRAID SAS HBA emulation support, allows local guest users to cause a denial of service (QEMU instance crash) via a crafted SCSI controller CTRL\_GET\_INFO command.

软件：QEMU

源码：hw/scsi/megasas.c

出现位置： 758-765行

关键源码：

memset(&info, 0x0, dcmd\_size);

if (cmd->iov\_size < dcmd\_size) {

trace\_megasas\_dcmd\_invalid\_xfer\_len(cmd->index, cmd->iov\_size,

dcmd\_size);

return MFI\_STAT\_INVALID\_PARAMETER;

}

.......

memcpy(info.product\_name, base\_class->product\_name, 24);

snprintf(info.serial\_number, 32, "%s", s->hba\_serial);

snprintf(info.package\_version, 0x60, "%s-QEMU", qemu\_hw\_version());

memcpy(info.image\_component[0].name, "APP", 3);

snprintf(info.image\_component[0].version, 10, "%s-QEMU",

base\_class->product\_version);

memcpy(info.image\_component[0].build\_date, "Apr 1 2014", 11);

memcpy(info.image\_component[0].build\_time, "12:34:56", 8);