CVE-2015-8666

描述：Heap-based buffer overflow in QEMU, when built with the Q35-chipset-based PC system emulator.

软件：QEMU

源码：hw/acpi/core.c

出现位置： 638-649行

关键源码：

void acpi\_gpe\_init(ACPIREGS \*ar, uint8\_t len)

{

ar->gpe.len = len;

ar->gpe.sts = g\_malloc0(len / 2);

ar->gpe.en = g\_malloc0(len / 2);

}

void acpi\_gpe\_reset(ACPIREGS \*ar)

{

memset(ar->gpe.sts, 0, ar->gpe.len / 2);

memset(ar->gpe.en, 0, ar->gpe.len / 2);

}