蓝牙耳机crash分析

1 问题描述

播放电视节目或是播放视频几天都ok，但是如果使用蓝牙耳机的话，过了一晚上就会出现系统重启的情况。

2分析过程：

因为重启了，没有保存log信息，所有需要想办法获取的log信息，包括dmesg，logcat等。

第一次进行log分析发现，出现了oom-killer，然后系统就重启了。比较明显，系统存在内存泄漏，最后触发了oom，从而导致系统重启。

于是，判断编写脚本，间隔抓取系统的内存使用情况以及剩余内存情况，主要是使用ps，top，free以及cat /proc/meminfo等工具。分析了抓取的log之后，发现在重启的时候，总的系统剩余内存还剩下120M左右。通过比对进程前后内存数据，也没有发现特别的进程内存增加的情况。

重新回头来分析oom-killer的logcat信息，发现gfp mask的标志为0x800d0，意味着申请page的空间为Zone\_NOMAL &Zone\_DMA。但是从log中可以看到DMA还是有page的。接着注意到一个细节，所有DMA page都是unreclaimable。而申请的page是需要claimable的。所以就出现了oom的情况。

由于申请的是low memory，所以可以断定是内核空间出现了内存泄漏。于是重点追查蓝牙的驱动代码。通过使用kmemcheck工具来最后定位到问题代码。

When Bluetooth headset connected to the TV platform, the platform must reboot when play music all night.

Because the platform has been reboot, all the log has lost.So the first important thing is to get the platform status before reboot and get logs such as logcat and dmesg and so on.

And first analysis the log, I found that oom-killer has happened and then the tv platform reboot. This means that there is memory leak in the system, but which module? So, I use some linux tools, like ps, cat /proc/meminfo, and free command to get the usage memory and free memory information every 5 minutes.

Unfortunately, before reboot, it still has more than100MB free memory. And I also can’t find the special memory consuming thread before platform reboot. But I have got an important information that as the low memory reduces to an fixed value, the platform will reboot immediately.

So I need to analysis the oom-killer log carefully. I found that the page flag gfp\_mask is 0x800d0, which means that the memory page just can be allocated from Zone\_Normal or Zone\_DMA. But I still can see that the Zone DMA has several pages can be used.

It’s must wrong somewhere. I notice that the remain free pages of Zone\_DMA are all unreclaimable. But the pages we want to requested are claimable. So the memory manager system think that there is no free memory, then the memory oom-killer happened.

As it wants to allocate page from low memory, I judged that there must have memory leak on the kernel space, and must hard relative to the Bluetooth device driver. And then we focus on the Bluetooth driver code. By used kmemcheck tool, finally we find the point that causes memory leak at kernel space.

【1】内存排除方法http://blog.csdn.net/xiangpingli/article/details/39623979

【2】Linux内核高端内存http://ilinuxkernel.com/?p=1013