一、Bluetooth Socket 通信层（应用层接口）

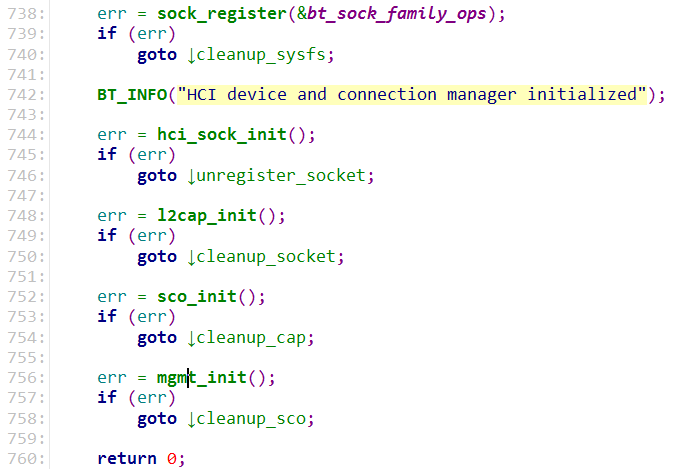
Bluetooth 驱动启动日志。



初始化bluetooth各个协议层套接字。

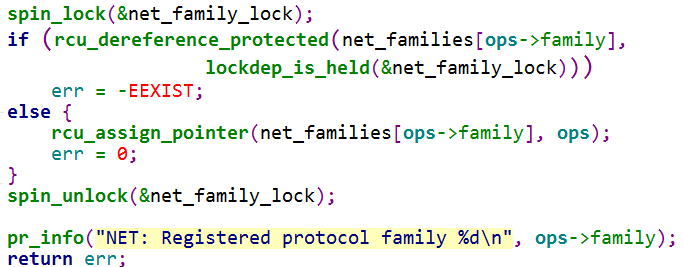
Net/Bluetooth/af\_bluetooth.c

static int \_\_init bt\_init(void)函数中关键初始化代码。



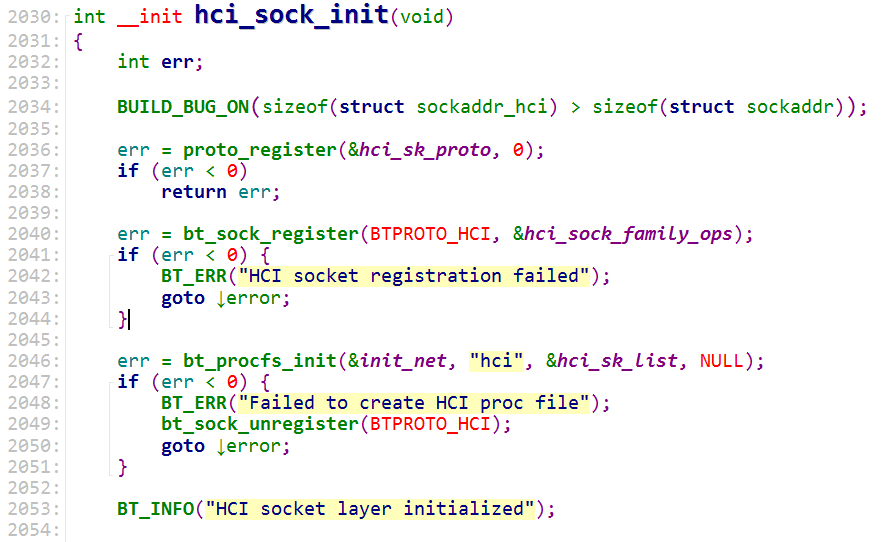
Bt\_sock\_family\_ops注册，初始化hci，l2cap，sco及mgmt。

Sock\_register(&bt\_sock\_family\_ops)函数实现：



将ops写入到net\_families全局数组中，完成注册。

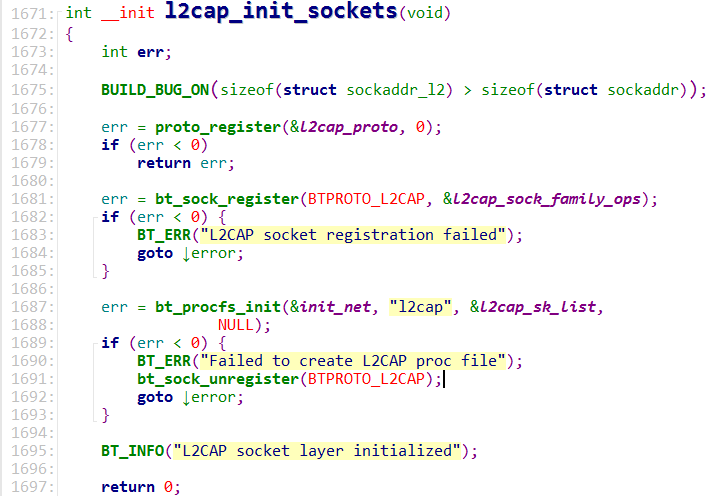
Hci\_sock\_init()函数初始化hci socket layer



L2cap\_init()函数实现如下：

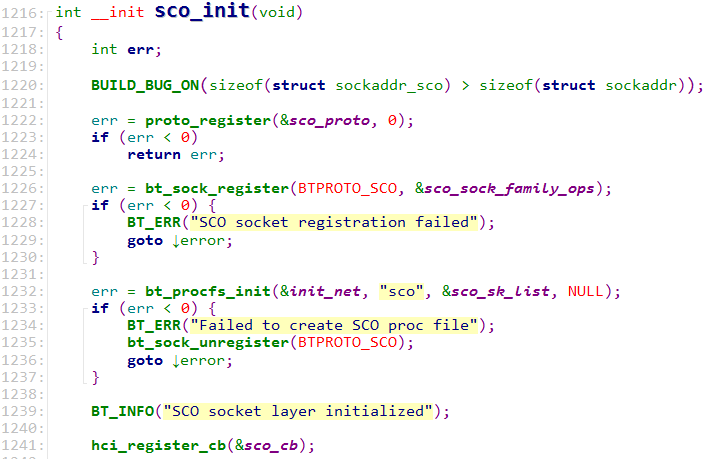


会调用l2cap\_init\_sockets函数初始化对应套接字协议。



然后调用hci\_register\_cb(&l2cap\_cb);初始化上层协议接口。

Sco\_init()函数

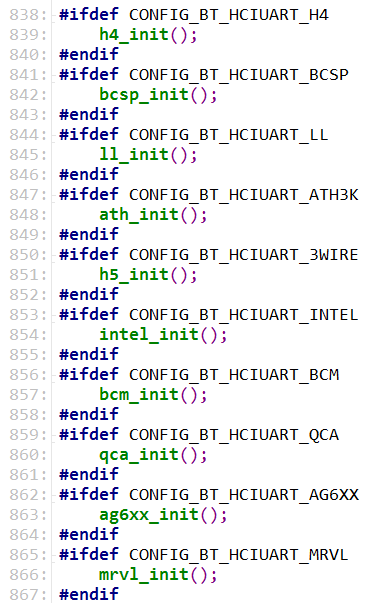


初始化SCO socket layer，并注册sco\_cb，初始化和hci协议层的接口。

二、HCI串口驱动初始化，接下来初始化hci uart驱动。Driver/Bluetooth/hci\_ldisc.c

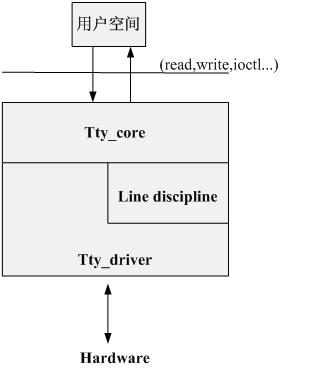


注册线路规程。注册完线路规程，开始根据内核配置，分别注册内核所支持的蓝牙HCI串口协议。HCI串口协议是连接硬件数据和应用层数据交互的桥梁。



三、tty框架和uart框架概念

在linux系统中，tty表示各种终端。终端通常都跟硬件想对应。tty框架层次结构图如下：



用户空间提供硬件操作接口，例如read，write等。用户空间主要是通过设备文件同tty\_core交互，tty\_core根据用户空间的操作类型再选择跟line discipline（线路规程）还是跟tty\_driver（serial\_core）交互。例如设置硬件的ioctl指令就直接交给serial\_core处理。Read和write操作就会交给line discipline处理。

四、概念性描述

蓝牙协议栈与蓝牙底层设备一般是通过串口连接，两者之间通过HCI协议通讯。这就要求实现一个串口tty驱动。而对于Bluez协议栈来说，它是通过建立蓝牙的socket来发送、接收数据。因此，在蓝牙通信中，对上层应用是socket通信，对底层则一般是通过一个tty驱动实现。

五，初始配置

一般来说，应用程序初始化并使用蓝牙设备的配置步骤如下：

1.    应用程序打开一个tty设备，该tty物理上与蓝牙芯片连接，两者之间使用HCI通信。

2.    调用该tty的ioctl，设置线路规程为N\_HCI。此时会调用到hci\_uart\_tty\_open函数。

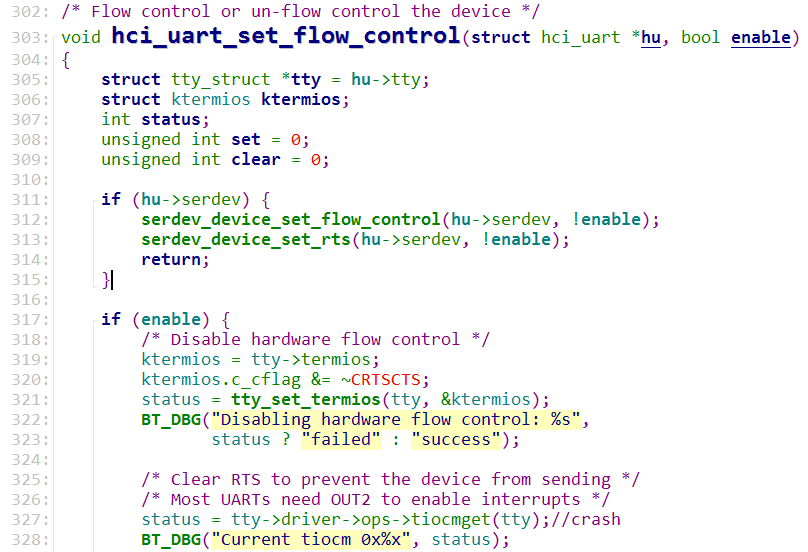
3.    调用IOCTL HCIUARTSETPROTO，设置proto，此ioctl最终会调用到N\_HCI线路规程中的hci\_uart\_tty\_ioctl函数。下文将详细讨论。

4.    应用程序打开蓝牙socket，发送、接收数据。这些数据在内核中最终会转到N\_HCI线路规程，并最终通过tty串口驱动与蓝牙芯片交互。

漏洞案例

CVE-2019-10207。漏洞类型，kernel NULL pointer dereference

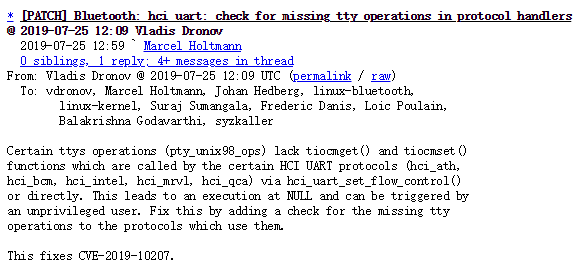
该漏洞出现在蓝牙HCI串口驱动中，具体漏洞函数是hci\_uart\_set\_flow\_control()。该函数是设置串口设备的流量控制的，实现如下：



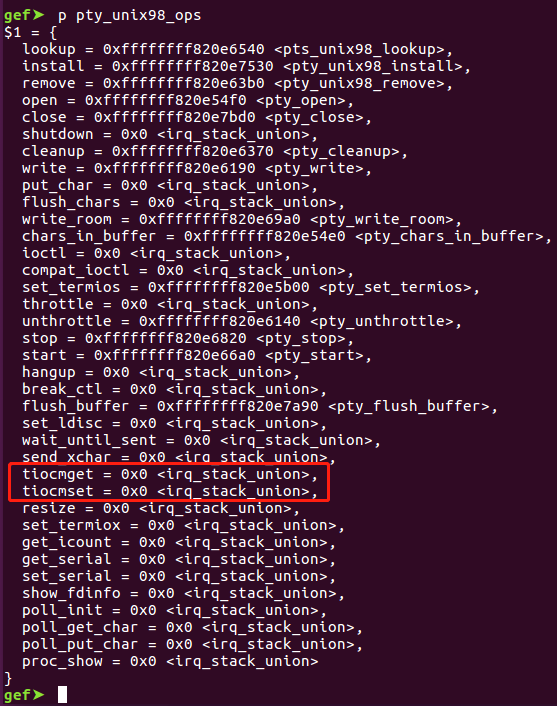
327行，调用tiocmget()函数时，发生空地址引用，说明tiocmget()函数为空。

理论上，tiocmget()是属于ops操作函数，正常情况下是不会为空的。但是在非正常情况下是不存在的。哪种情况？

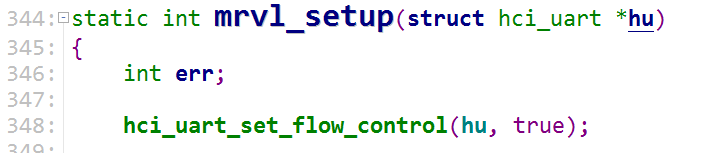
在该漏洞的补丁中可以找到答案。



该段话意思是，如果tty终端为pty时，pty为虚拟终端（伪终端），tiocmget()和tiocmset()这两个操作都是不支持的，故函数指针都是为空。

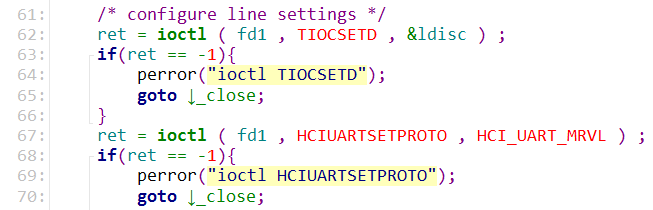


因此，只要是将ptyh和hci串口协议绑定的话，就会有机会调用tiocmget/tiocmget函数并触发漏洞。CVE-2019-10207漏洞细节中，作者提供的崩溃栈回溯是较为便捷的触发方式，毕竟是自动fuzz出来的。调用路径如下:

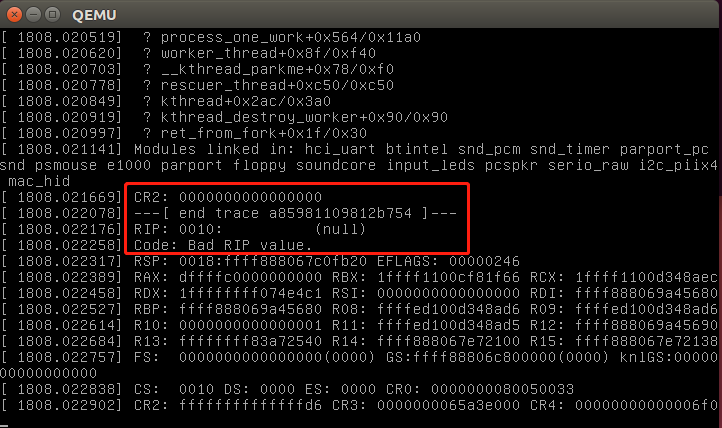


Mrvl是表示Marvell公司提供的蓝牙芯片接口。将pty终端和mrvl协议绑定时，就自动调用mrvl\_setup函数，进而触发漏洞。

还原poc。



触发漏洞，如下图。



Poc：<https://github.com/butterflyhack/CVE-2019-10207>