bthport.sys Elevation of Privilege Vulnerability

## surroundings

Microsoft Windows full version

## Vulnerability description

Because Bthport.sys!HCI\_GetLocalServiceKey does not determine whether the user has the right to create the registry in the current context when processing the user's IOCTL, resulting in arbitrary registry creation and local privilege escalation

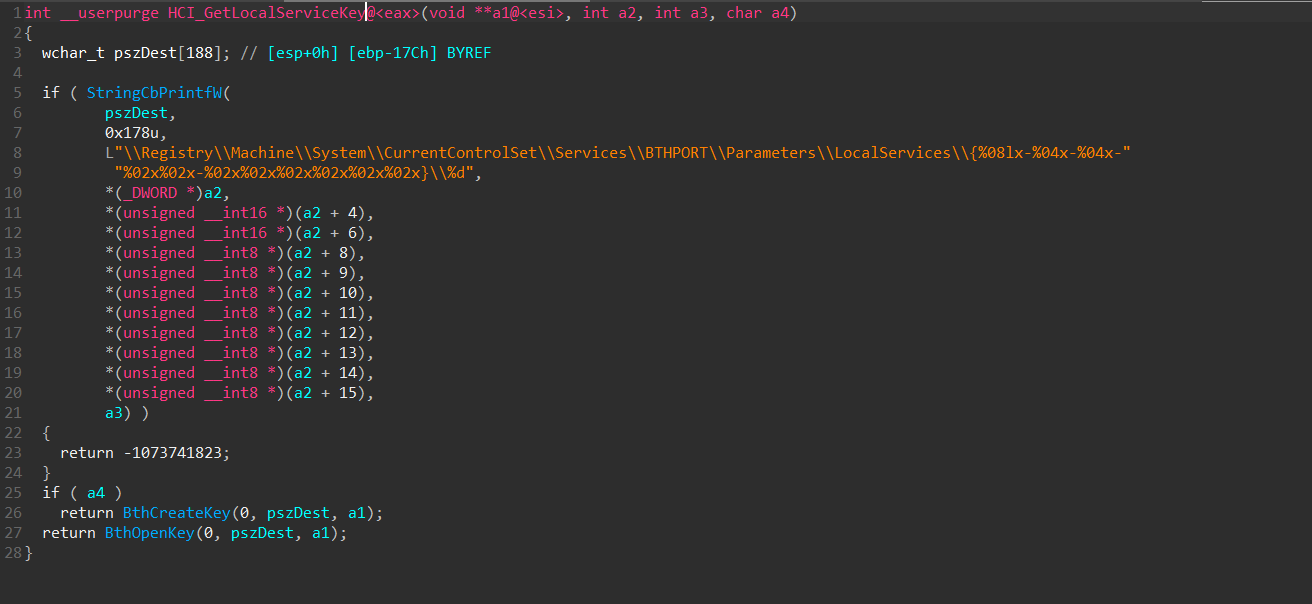
## **Vulnerability root cause**

Bthport.sys is a bluetooth driver for windows. When the computer has a bluetooth adapter, the system will create a device symbolic link

which is used by the bluetooth API (https://docs.microsoft.com/en-us/windows/win32 /api/\_bluetooth/) and make an IOCTL call to Bthport.sys

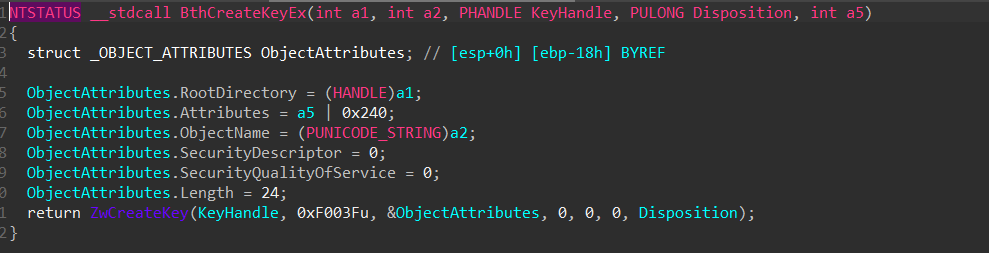
When the user calls the IOCTL as 0x41104C, the driver will call HCI\_SetLocalServiceInfo and hit the vulnerability function HCI\_GetLocalServiceKey

The IOCTL has the FILE\_ANY\_ACCESS permission, however as Everyone has this permission on the symbolic link



As shown in the figure above, HCI\_GetLocalServiceKey will create a subkey in HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\BTHPORT\Parameters\LocalServices, and create a subkey on this item

When calling ZwCreateKey The handle is from user mode, the problem here is that the OBJ\_FORCE\_ACCESS\_CHECK flag is not added to force an access control check, as shown in the image below



It is not necessarily a problem to create a subkey under HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\BTHPORT\Parameters\LocalServices. The problem is that a subkey is created under the subkey, and these two subkeys are named controllable, it is IRP .AssociatedIrp.MasterIrp

When a subkey is created, since the subkey is created in the current user context, the subkey has full control permissions for the current user context. If we create a registry symbolic link under the subkey (only KEY\_CREATE\_LINK is required) |KEY\_CREATE\_SUB\_KEY), the create registry operation will create the key linked by the registry symlink

## EXP

My exploit workflow:

1.Determine whether the Fax service registry key is completely controllable to the current user. If it is completely controllable, then starting the Fax service is to start the interactive application cmd.exe that creates system permissions by itself

2.If the fax service registry key is uncontrollable, it means that it has not been used, then first create a powershll process and pass the command to turn on bluetooth (in order to test whether there is a bluetooth adapter and the system is stable)

3.Make a DeviceIoControl call for each device symlink traversed and send 0x41104C IOCTL, once HCI\_SetLocalServiceInfo is called, HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\BTHPORT\Parameters\LocalServices\{00001103-0000-1000-8000-00805f9b34fb}\1094795585 will be was created

4.Delete the HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\BTHPORT\Parameters\LocalServices\{00001103-0000-1000-8000-00805f9b34fb}\1094795585 key and recreate a registry symlink named HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\Group Policy\State\Machine\GPO - List\34

5.Make another DeviceIoControl call with the found wireless device link handle, HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\GPO - List\34 will be created

6.Then we create subkey 123 registry symlink under HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\Group Policy\State\Machine\GPO - List\34 and link to HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Fax key

7.Execute the cmd gpupdate/force command to update the group policy. At this time, the group policy process will run with system privileges and delete all registry subkeys under HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\GPO - List, So the registry symlink 123 we created to link the fax service item and subkeys will be deleted

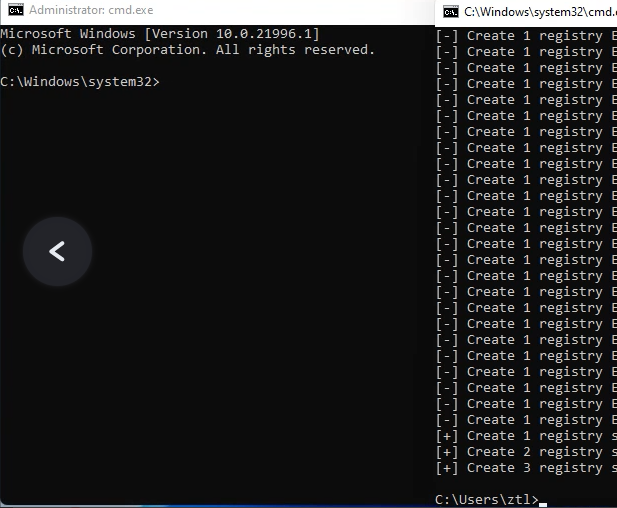
8.Since the execution of the group policy will block, in order to use the speed, a new thread is created for subsequent use. In another thread, it will always judge whether the fax service item exists. If the fax service item does not exist, it means that it has been deleted by the group policy. Then we make the DeviceIoControl call again to exploit the vulnerability to create HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Fax, at this time we have full control over the service registry key

9.Modify the ImagePathfax service item to tracing\exp.exe, and move itself to C:\Windows\tracing\exp.exe (this service has event tracing environment variables, C:\Windows\tracing is writable by ordinary users), Then run the cmd command sc start Fax, and the process itself will start again with system privileges

1. The own process started with system permissions will judge whether the current fax registry service item is completely controllable. If it is completely controllable, open the winlogon process token of the current session, and call CreateProcessAsUser to create a cmd process display with system permissions, and finally delete itself and restore fax Security properties of the registry service key

My build environment: Visual Studio 2019

The result of successful execution of exp: As shown in the figure below, the system permission cmd is popped up



Exp failed execution result: cmd is not popped up, please check whether the vm virtual machine shares bluetooth and whether the computer has a bluetooth adapter, this is a necessary condition. Another possibility is that the fax service is already running, if this is the case in the competition environment, please let me know and I will change the utilization method.

## 17 issues related to the answer

1.Does each entry defeat the target's techniques designed for the safe execution of code (ASLR, DEP, Sandboxing, etc)?

The exploit bypasses all memory-based mitigations, but there are registry symlink mitigations, so the exploit can only be successfully exploited on medium permissions

2.If the exploit is successful, how do you plan to prove it?

My exploit will pop up a cmd process with system privileges and can execute arbitrary commands on that command window

3.Does your entry require any user interaction beyond what is required to initiate the attempt?

No user interaction required

4.Did you know that in a 30 minute period you have 3 5 minute attempts to run your entry and destroy the goal?

Yes, I know, I followed the game

5.Is your entry done in a user session? We don't reboot the device or log it in and out.

Yes, the exploit can be exploited without rebooting

6.Is there an initial vulnerability in the registered target? Are there sandbox escapes (if required) in the registered target? If you are registering for the local privilege escalation category, did you know that the vulnerability must exploit a kernel vulnerability (rather than a vulnerability in a system service, a misconfigured application, etc.)?

The vulnerability is a local elevation of privilege vulnerability in the kernel driver, not in a printer or system service

7.Do any of your entries require a man-in-the-middle attack to be successful? If so, please provide step-by-step instructions on how you would like to configure your environment.

without any middleman

8.Do any of your entries require an authentication bypass in the target to be successful?

No authentication required

9.How many vulnerabilities are being exploited in each of your entries?

There is only one vulnerability, I only participate in the Windows 11 local privilege escalation class

10.Are any of the vulnerabilities known, published, or been reported to the vendor (or be considered n-day vulnerabilities)?

The vulnerability is not reported to any vendor, it is 0day

11.Are you aware that a whitepaper describing the attack is required to be delivered with your entry?

yes, i know, and am doing it

12.Do you have any additional questions about the rules?

No problems, previous email communication was pleasant and satisfying

13.Which company/team are you representing or are you independent?

individual

14. If you are company or a team, who are researchers that are working on the entries?

I'm a competing security researcher

15. What is your researcher account username?  If you don’t have one, please open an account and notify us of the account username.

T0

16.How do you want to be attributed in the blogs, advisories, and press?

Security researcher named T0 successfully breached the target

17. Do you plan on attending in person or remotely?

Remote competition