# PENTESTING REPORT

## PWNKIT CVE-2021-4034
## CVE-2021-41773/42013

*Submitted by:*

Muhammad Fatiq

*Submitted to:*

*Muhammad Bilal*

TABLE OF CONTENT:



# Vulnerability 1:

# PWNKIT 2021-4034:

## OVERVIEW:

CVE-2021-4034, commonly known as "PwnKit," is a critical privilege escalation vulnerability in the pkexec component of the ) framework, which is used across many Linux distributions. Discovered in January 2022, this flaw allows an unprivileged local user to gain root access on a vulnerable system due to improper handling of environment variables. Exploiting this vulnerability can enable an attacker to execute arbitrary code with elevated privileges, potentially compromising the entire system. To address the issue, users should update Polkit to the latest patched version or apply available security patches to mitigate the risk.

## KEY INFORMATION:

| Attribute | Details |
|---|---|
| CVE Identifier | CVE-2021-4034 |
| Common Name | PwnKit |
| Vulnerability Type | Privilege Escalation |
| Component Affected | pkexec (part of Polkit) |
| Impact | Allows local unprivileged users to gain root access |
| Exploit | Exploits improper handling of environment variables |
| Affected Systems | Various Linux distributions using vulnerable Polkit versions |
| Risk Value | High (CVSS v3.1 Base Score: 7.8/10) |
| Mitigation | Update Polkit to the patched version or apply security patches |

## HOW IT WORK:

The PwnKit exploit (CVE-2021-4034) operates by taking advantage of a flaw in the pkexec utility, which is part of the Polkit framework on Linux systems. The vulnerability arises from improper handling of environment variables by pkexec. An attacker with local, unprivileged access can set malicious environment variables that pkexec does not properly validate or sanitize. When pkexec is executed with these crafted variables, it can be tricked into executing arbitrary commands with root privileges. This allows the attacker to escalate their privileges and gain full control over the system. The exploit essentially leverages the way pkexec handles the environment to bypass normal security restrictions and achieve unauthorized access.

## IMPACT:

Certainly! Here's a more detailed explanation of the key impacts of the PwnKit exploit (CVE-2021- 4034):

### Privilege Escalation:

The exploit allows a local user with minimal or no privileges to elevate their access level to root. This means that an attacker who is not an administrator can gain full control over the system.

### System Compromise:

Once root access is achieved, the attacker can fully control the system. This includes installing and executing malicious software, modifying or deleting system files, and accessing all user data.

### Potential for Widespread Exploitation:

The vulnerability affects a wide range of Linux distributions that use the vulnerable version of Polkit. This broad impact increases the risk of widespread exploitation across many systems.

### Loss of Data Integrity and Confidentiality:

The attacker can alter or delete files, which compromises the integrity of the system and its data. Additionally, they can access sensitive information, leading to potential data breaches and unauthorized access to confidential information.

## HOW CAN ACCESS IT:

An attacker can gain unauthorized access to a system due to the PwnKit vulnerability (CVE-2021- 4034) by exploiting the improper handling of environment variables in the pkexec command.

Initially, the attacker needs local, unprivileged access to the system. They then craft specific environment variables designed to exploit the flaw in pkexec. When pkexec is executed with these manipulated variables, it fails to properly sanitize or validate them, which can lead to unintended behavior. This flaw allows the attacker to execute arbitrary commands with root privileges, bypassing normal security restrictions. As a result, the attacker gains full control over the system, including the ability to modify system files, install malicious software, and access or alter sensitive data.

```
tryhackme@pwnkit:~/pwnkit$ ls
README.md  cve-2021-4034-poc.c
tryhackme@pwnkit:~/pwnkit$ cat README.md
# CVE-2021-4034
PoC for PwnKit: Local Privilege Escalation Vulnerability in polkit
's pkexec (CVE-2021-4034)

https://seclists.org/oss-sec/2022/q1/80
https://blog.qualys.com/vulnerabilities-threat-research/2022/01/25
/pwnkit-local-privilege-escalation-vulnerability-discovered-in-pol
kits-pkexec-cve-2021-4034
```

```
tryhackme@pwnkit:~/pwnkit$ ^C
tryhackme@pwnkit:~/pwnkit$ gcc cve-2021-4034-poc.c  -o exploit
tryhackme@pwnkit:~/pwnkit$ ls
README.md  cve-2021-4034-poc.c  exploit
tryhackme@pwnkit:~/pwnkit$ file exploit
exploit: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), d
ynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildI
D[sha1]=f0dd6e4158847042c42c0c8f3ada4e4213e15f0a, for GNU/Linux 3.
2.0, not stripped
tryhackme@pwnkit:~/pwnkit$ ./exploit
# whoami
root
# ls
README.md  cve-2021-4034-poc.c  exploit
# cd /root
# ls
flag.txt  snap
# cat flag.txt
THM{CONGRATULATIONS-YOU-EXPLOITED-PWNKIT}
# THM{CONGRATULATIONS-YOU-EXPLOITED-PWNKIT}THM{CONGRATULATIONS-YOU
-EXPLOITED-PWNKIT}
```

## PATCHING:

To patch the PwnKit vulnerability (CVE-2021-4034), follow these steps:

**Identify Your System**:

Determine your Linux distribution and version to find the right package updates.

**Update Polkit**:

**Debian/Ubuntu**: sudo apt update && sudo apt upgrade polkit

**Red Hat/CentOS**: sudo yum update polkit

**Fedora**: sudo dnf update polkit **Arch Linux**: sudo pacman -Syu polkit **Verify the Update**:

Check the Polkit version with pkexec --version to ensure it's updated.

**Restart Services**:

Reboot your system or restart relevant services to apply the update.

**Monitor Advisories**:

Keep up with security advisories for further updates.

These steps will secure your system against the PwnKit vulnerability.

### CONCLUTION:

In conclusion, the PwnKit vulnerability (CVE-2021-4034) in Polkit's pkexec utility allows local unprivileged users to escalate their privileges to root by exploiting improper handling of environment variables. This critical flaw poses a significant security risk as it enables attackers to gain full control over affected systems. Promptly updating Polkit to the latest version is essential to mitigate this vulnerability and protect systems from potential compromise.

.....

## Vulnerability 2:

## CVE-2021-41773-41013:

### OVERVIEW:

CVE-2021-41773 is a path traversal vulnerability in Apache HTTP Server versions 2.4.49 and 2.4.50.

This flaw allows attackers to access files outside the intended web root directory by exploiting

improper validation of file paths. As a result, sensitive files on the server's filesystem could be exposed. Discovered in October 2021, the vulnerability can potentially lead to unauthorized access to critical data if not addressed. Users are advised to upgrade to Apache HTTP Server 2.4.51 or later to mitigate this risk.

### KEY INFORMATION:

| Attribute | Details |
| --- | --- |
| CVE Identifier | CVE-2021-41773 |
| Vulnerability Type | Path Traversal |
| Affected Versions | Apache HTTP Server 2.4.49 and 2.4.50 |
| Discovery Date | October 2021 |
| Impact | Allows unauthorized access to files outside the web root directory |
| Mitigation | Update to Apache HTTP Server 2.4.51 or later |
| Risk Rate | High (CVSS v3.1 Base Score: 7.5/10) |

## HOW IT WORK:

CVE-2021-41773 is a path traversal vulnerability in Apache HTTP Server versions 2.4.49 and 2.4.50 that allows attackers to access files outside of the designated web root directory. The exploit involves crafting HTTP requests with specially designed path traversal sequences (such as ../) that bypass the server's directory restrictions. When the server processes these requests, it fails to properly validate and sanitize the file paths, granting unauthorized access to sensitive files and directories that should not be exposed. This can lead to the leakage of critical information, such as configuration files and logs, which could be used for further exploitation or compromise of the system.

## IMPACT:

The impact of CVE-2021-41773 is significant, as it allows unauthorized access to sensitive files on a server due to a path traversal vulnerability in Apache HTTP Server versions 2.4.49 and 2.4.50. By exploiting this flaw, attackers can bypass directory restrictions and access files located outside the intended web root directory. This can lead to the exposure of critical information, such as server configuration files, access logs, or other sensitive data, which could be used to further compromise the server or gain deeper access to the system. The vulnerability thus poses a high risk, potentially leading to information leakage, data breaches, and increased security risks if not properly mitigated.

## HOW TO ACCESS IT:

To exploit CVE-2021-41773, an attacker with access to the server can craft a malicious HTTP request that includes directory traversal sequences, such as ../, to navigate outside the web root directory. By sending this specially crafted request to the Apache HTTP Server, the attacker can bypass the server's directory restrictions due to improper validation of file paths. This exploitation allows the attacker to access files and directories that should otherwise be restricted. The attacker can use this method to view or download sensitive files, such as configuration files, logs, or other critical data, potentially leading to further exploitation or compromise of the server.

APACHAE VERSION 2.4.49:

ACCESS WHEN CGI IS NOT ENABLE:


WHEN CGI IS ENABLE:


## PATCHING:

To patch CVE-2021-41773, administrators should upgrade their Apache HTTP Server to version

2.4.51 or later, where the vulnerability has been addressed. This update involves downloading and installing the latest version of Apache HTTP Server from official repositories or the Apache website. System administrators should first check their current version and then apply the update using their package management system, such as `apt` for Debian/Ubuntu, `yum` for Red Hat/CentOS, or `dnf` for Fedora. After applying the update, it is advisable to restart the Apache service or reboot the server to ensure that the changes take effect. Regularly checking for and applying updates is crucial to maintaining security and protecting against vulnerabilities.

## CONCLUTION:

In conclusion, CVE-2021-41773 represents a critical path traversal vulnerability in Apache HTTP Server versions 2.4.49 and 2.4.50, which allows attackers to bypass directory restrictions and access sensitive files outside the intended web root. This exposure can lead to significant security risks, including unauthorized access to configuration files and other critical data, potentially facilitating further attacks or breaches. To mitigate this vulnerability, it is essential to upgrade to Apache HTTP Server version 2.4.51 or later, which includes fixes for this issue. Regular updates and vigilant system

maintenance are crucial in safeguarding against such vulnerabilities and ensuring the security of web server environments.

.....