Escalate Privileges by Exploiting Vulnerability in pkexec

ILABS

CEH PRACTICAL

Polkit or Policykit is an authorization API used by programs to elevate permissions and run processes as an elevated user.The successful exploitation of the Polkit pkexec vulnerability allows any unprivileged user to gain root privileges on the vulnerable host.

In the pkexec.c code, there are parameters that doesn't handle the calling correctly which ends up in trying to execute environment variables as commands. Attackers can exploit this vulnerability by designing an environment variable in such a manner that it will enable pkexec to execute an arbitrary code.

Aim

We will use a proof-of-concept code to execute the attack on the target system and escalate the privileges from a standard user to a root user. we will be exploiting the pkexec CVE-2021-4034 vulnerability

DEMO

THANKS