

1Q. Explores on CVE-2021-4034

Ans:- CVE-2021-4034 is a vulnerability in polkit's pkexec that allows an unauthorized user to gain root access to a Linux system. The vulnerability is due to the pkexec tool's improper handling of command-line arguments.

The exploitation of CVE-2021-4034 requires local authenticated access to the vulnerable machine and can't be run remotely without such authentication. The most likely attack scenario is from an internal threat where a malicious user can escalate from no privileges to full root privileges.

An external attack scenario would be from an attacker who already had local authenticated access to the vulnerable system either from another vulnerability (or) password spraying style attack. Once local authenticated access is achieved, the external attacker could then escalate to full root privileges through this vulnerability.

2100031921

Proof of Concept (Poc) exploit Code has been made publicly available for CVE-2021-4034 and security researchers have tested and confirmed the validity of this exploit.

\* CVE-2021-4034 is a vulnerability.

### Fix the polkit privilege Escalation

The Qualys research Team has disclosed a 12-year old memory corruption vulnerability in polkit's pkexec. The vulnerability is tracked as CVE-2021-4034 allows any unprivileged user to ~~login~~ gain full root privileges on a vulnerable Linux machine.

The research team confirmed that it has successfully tested this vulnerability on ubuntu, Debian, fedora and CentOS with the default configuration - since polkit is part of the default packages on most Linux distributions, we can say that the whole Linux community is under threat. It is essential to fix the CVE-2021-4034 vulnerability as the flaw is being exploited in the wild.



Impact:-

- 1) Bypass authentication checks
- 2) Execute arbitrary code with elevated privileges
- 3) Gain root access to a Linux system.
- 4) Perform malicious activities.

Path:-

- 1) A patch is available for this vulnerability.
- 2) You should immediately upgrade your systems to the latest version.
- 3) There is also a workaround that functions as a stop-gap while you evaluate your systems and perform necessary patches and upgrades.

Exploiting the vulnerability

- 1) requires local authenticated access to the vulnerable machine
- 2) Can't be run remotely without such authentication

CVSSv3 base score

Calculated to be a high 7.8 out of 10.0