CyMinded Security Report

Subject Matter: CVE-2021-4034

CVE-2021-4034 \ Polkit Pkexec Overview

Also known as **PwnKit**, is a local privilege escalation vulnerability that was found on the polkit's pkexec utility.

Polkit's pkexec is a SUID-root program, that allows an authorized user to execute program as another user – unprivileged users can run commands as a privileged users according to predefined policies, in case the *username* is not specified, then the program will be executed as the **root** (SIUD permission guidelines).

The vulnerability, which was found by Qualys's Researchers is a memory corruption vulnerability, pkexec version didn't handle the calling parameters count correctly which can lead to the execution of environment variables as commands,

An attacker might leverage this by making environment variables execute arbitrary code that runs with root privilege.

The Bug's Cause: In pkexec, the main() function gets argc and argv[] as arguments but does not validate input when argc=0 and argv=[{NULL}], this edge case is possible to trigger with an empty argv[] array. Since execve() looks for the new program's path, the function sets the program path and argv[1] to an out-of-bounds memory location.

The out-of-bounds memory location is the next value on the stack, which is part of the environment variables (envp[]) passed by execve(), as argv[] and envp[] are stored contiguously, it allows the path to be set to a malicious environment variable executable, for example, an attacker could inject a malicious executable as the PATH environment variable still in user mode, and envp[0] would access it during execution of pkexecve().

This can lead to the execution of arbitrary code and have a serious effect, as we discussed, pkexec is used to allow executing programs as root.

Privilege escalation is quite dangerous, as it allows to perform critical system processes or even compromise the entire system by performing various malicious activities.

CVSS Score: 7.8 - HIGH, it effects Unix like Linux distributions e.g. Debian, Ubuntu, Fedora and CentOS etc., since the vulnerability goes back to pkexec first version in 2009, the assumption was that all Linux distributions with default configuration were vulnerable.

Potential Attacker Identity: as this attack is granting root privileges, we assume that the attacker already has local access, it might be an employee or an attacker who got employee credentials which can potentially be anyone.

This vulnerability is very powerful and because of that the identification and motivation of the attacker may vary, it might be an APT group that wishes to deficit a system of a certain company, it might be theft of customer data and more, the point is, that by having root privileges there are endless possibilities to what can be achieved and done.

Mitigation And Prevention: patches that set validation checks to the pkexec utility's command line arguments exist and systems that have Polkit installed are recommended to be updated to the latest version as soon as possible.

With that, it is recommended to set pkexec utility access restrictions, and add systems logs monetization too, as it is a sensitive and powerful tool by core.