Hive Pro

THREAT ADVISORY

PwnKit vulnerability affects major Linux distributors

TA2022018

Threat Level RED

Publish Date – Jan 26, 2022

PwnKit is a local privilege escalation vulnerability discovered in polkit's pkexec, an SUID-root program that is installed by default on every major Linux distribution.
This vulnerability can be easily exploited due to following

- All major Linux distributions include pkexec by default.
- Since its beginning in May 2009, pkexec has been vulnerable.
- This vulnerability can be exploited by any unprivileged local user to gain full root privileges.
- Even though this vulnerability is technically a memory corruption, it can be exploited instantly, reliably, and in an architecture-independent manner.
- It can be exploited even if the polkit daemon is not running.

This vulnerability is been widely exploited after researchers have disclosed PoC. Official patch for PwnKit can be downloaded from link below. As all Linux distributions use pkexec and only few have released patches for this vulnerability for there operating system(OS)and organizations can remove the SUID-bit from pkexec as a temporary mitigation until official patches of all Linux distributors are released.

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-4034	Polkit versions from 2009	cpe:2.3:a:polkit:polkit:*:*:*:*:*:*:*:*	Local Privilege Escalation Vulnerability in polkit's pkexec (PwnKit)	CWE-284, CWE-787, CWE-125

Patch Links

https://gitlab.freedesktop.org/polkit/polkit/-/commit/a2bf5c9c83b6ae46cbd5c779d3055bff81ded683
https://www.debian.org/security/2022/dsa-5059
http://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.434679
https://www.suse.com/support/update/announcement/2022/suse-su-20220189-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220190-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220191-1/
https://www.debian.org/lts/security/2022/dla-2899
https://oss.oracle.com/pipermail/el-errata/2022-January/012089.html
https://oss.oracle.com/pipermail/el-errata/2022-January/012086.html
https://oss.oracle.com/pipermail/el-errata/2022-January/012084.html

References

https://blog.qualys.com/vulnerabilities-threat-research/2022/01/25/pwnkit-local-privilege-escalation-vulnerability-discovered-in-polkits-pkexec-cve-2021-4034
https://access.redhat.com/security/cve/CVE-2021-4034
https://ubuntu.com/security/CVE-2021-4034