SECURITY ALERT

Cyber Defense Intelligence

January 27, 2022

SECURITY ALERT: Vulnerability could allow unprivileged users to gain root privileges via default configuration on Linux

Overview:

This week, it was reported that a memory corruption vulnerability, tracked as CVE-2021-4034, was discovered in Polkit's pkexec – a SUID-root program installed by default on every major Linux distribution. CVE-2021-4034, also known as PwnKit, could allow unprivileged users to gain root privileges on the vulnerable host by exploiting it in its default configuration.

The vulnerability was discovered in November 2021 by the Qualys Research Team but was not disclosed to the public until January 25, 2022, via a coordinated disclosure with both vendor and open-source distributions. The researchers at Qualys were able to independently verify the vulnerability, develop the exploit, and obtain full root privileges on default installations of Ubuntu, Debian, Fedora, and CentOS. There are also other Linux distributions that are likely to be vulnerable and exploitable. While Qualys did not release the exploit publicly, they provided enough technical detail for others to recreate it.

According to Bharat Jogi, Qualys' Director of Vulnerability and Threat Research, Polkit controls system-wide privileges in Unix-like operating systems and provides an organized way for non-privileged processes to communicate with privileged processes. One can also use Polkit to execute commands with elevated privileges using the command pkexec followed by the command intended to be executed (with root permission). This means that pkexec allows an authorized user to execute commands as another user. If a username isn't specified, the command to be executed will be run as the administrative super user (root).

Hiding in plain sight for 12 years, PwnKit affects all versions of pkexec dating back to the first version from May 2009 (commit c8c3d83, "Add a pkexec(1) command"). Pillar Technology Partners recommends that users apply patches for PwnKit as they become available. Qualys will release the detections (QIDs) on their website as they become available, starting with vulnsigs version VULNSIGS-2.5.87-2 and in Linux Cloud Agent manifest version lx_manifest-2.5.387.2.1. Since pkexec is installed by default on most Linux systems and the vulnerability is exploitable in pkexec's default configuration, Linux systems should be assumed to be vulnerable until patched or mitigated.

Pillar Technology Partners' Recommendations:

Please apply the appropriate patches as soon as they become available.

If no patches are available for your operating system, you can remove the SUID-bit from pkexec as a temporary mitigation; for example: # chmod 0755 /usr/bin/pkexec

Users that want to look for signs of PwnKit exploitation can do it by checking the logs for either "The value for the SHELL variable was not found the /etc/shells file" or "The value for environment variable […] contains suspicious content." entries. Refer to the SIGMA rule below.

Ubuntu has released temporary mitigations and updates for PolKit to address the vulnerability in versions: 14.04 and 16.04 ESM (extended security maintenance). As well as versions 18.04, 20.04, and 21.04. Users need to run a standard system update and then reboot the computer for the changes to take effect.

Red Hat has also released temporary mitigations updates for Polkit on Workstation and on Enterprise products for supported architectures and extended life cycle support, TUS and AUS.

Indicators of Compromise (IoCs):

MD5sum

361f79031dd61b56a6d352d5640ec08a pwnkit.c

4cd09130cbe69df24e7ab80f6d2b48a7 pwnkit

sha256sum

19766c7da5202548e92b7bee2f48c6bbb4a4dd44bb214ed1eb36656a27b008a0 pwnkit.c

c2ac768a8a1ffd5d99dd539c7aed8b626b804e5986797ec4ef3d88b4c6de1811 pwnkit

sha1sum

ced0ff14fd053db32d5126905b9f73ea6ea47183 pwnkit.c

ddf4b822c5a4004aa3ae9244a55ae490330e9fcf pwnkit

How Pillar Technology Partners is Protecting our Clients:

Pillar Technology Partners offers VMaaS to provide a deeper understanding and control over organizational information security risks. If your enterprise is facing challenges with the scope, resources, or skills required to implement a vulnerability management program with your team, outsourced solutions can help you bridge the gap.

Ensure a SIM or SIEM LogRhythm, Microsoft Azure Sentinel, or AlienVault, combined with endpoint protection such as Sophos.

Other Helpful Resources:

- Past alerts and briefings from Pillar's Cyber Defense Intelligence Team
    - https://www.ptechcyber.com/intel-briefings
- Other resources on ptechcyber.com
    - https://www.ptechcyber.com/