Pkexec pwnkit vulnerability

1/31/2022

Summary

On January 26th 2022, Cambium Networks became aware of a serious vulnerability in polkit's pkexec utility dentified as CVE-2021-4034(pwnkit) and detailed in https://nvd.nist.gov/vuln/detail/CVE-2021-4034. The current version of pkexec doesn't handle the calling parameters count correctly and ends trying to execute environment variables as commands. An attacker can leverage this by crafting environment variables in such a way it will induce pkexec to execute arbitrary code. When successfully executed the attack can cause a local privilege escalation given unprivileged users administrative rights on the target machine.

This advisory only lists Cambium Networks products and services that are known to include the impacted software component and thus may be vulnerable. Products and services that do not contain the impacted software components are not vulnerable and therefore are not listed in this advisory. Because this is an ongoing investigation, be aware that products that are currently considered not vulnerable may subsequently be considered vulnerable as additional information becomes available.

Affected Products

1. cnMaestro On-Premises OVA and AMI version 2.4 or less. We have released cnMaestro patch 2.4.2-r31 to address this vulnerability. Customers using this version can download this patch from our support center at https://support.cambiumnetworks.com/files/cnmaestro/

2. **cnMaestro On-Premises AMI version 3.0.x.** We have released CnMaestro patch 3.0.4-r8 to address this vulnerability. Customers using this version can download this patch from our support center at https://support.cambiumnetworks.com/files/cnmaestro/

What actions should be taken

Customers who are running older version of CnMaestro On-Premises or unable to patch their system can perform the following action to mitigate from this vulnerability.

Run the following command from the VM shell:

```
[ -f /usr/bin/pkexec ] && sudo chmod 0755 /usr/bin/pkexec 2>/dev/null && echo "Pwnkit workaround set (SUID Bit removed)" || echo "Not vulnerable (pkexec not found)"
```