# Array Networks Security Advisory: Linux PwnKit vulnerability (CVE-2021-4034)

**Advisory Date: January 28, 2022**

Severity: Critical

## Overview

About Polkit for Linux:

Polkit (formerly PolicyKit) is a component for controlling system-wide privileges in Unix-like operating systems. Its main function is to allow non-privileged processes to communicate with privileged processes. The polkit can also be used to execute commands with elevated privileges using the pkexec utility followed by the command intended to be executed (with root permission).

About PwnKit Vulnerability:

A local privilege escalation vulnerability was found on polkit's pkexec utility. Successful exploitation of this vulnerability allows any unprivileged user to gain root privileges on the vulnerable host. Security researchers have independently verified the vulnerability, developed an exploit and obtained full root privileges on default installations of Ubuntu, Debian, Fedora, and CentOS. Other Linux distributions are likely vulnerable and probably exploitable.

## Impact

Array's **AVX, APV, AG, ASF, and AMP** Series products are **not** affected by this vulnerability.

Although the products are not affected, it is a good practice to control remote access to the systems. There are commands that can be used to limit SSH/WebUI access to trusted clients. Please refer to the individual product application guide for details or contact Array Networks Support via phone or e-mail.

AMP is not affected by CVE-2021-4043. However, since AMP runs as an application on the client OS, we suggest customers strengthen their server OS to avoid any issues.