CVE-2024-6387

Cambium Networks is aware of CVE-2024-6387 (https://www.qualys.com/2024/07/01/cve-2024-6387/regresshion.txt) and is currently investigating its impact on individual product lines. We can confirm that cnMaestro Cloud and XMS Cloud are not affected by this vulnerability.

The cnMatrix line of switches from firmware version 5.0.1-r4 may be vulnerable. Earlier versions are not impacted. If you are running firmware version 5.0.1-r4 or above, we recommend disabling ssh management for any switches and managing via cnMaestro. To disable SSH on cnMatrix:

- **cnMaestro**: In switch group configuration under "Management", unselect SSH, save and then sync configuration
- **Web UI**: Under System > SSH set SSH Status to "Disable" and then save config
- **Console**: (note this should not be done over ssh)
    - `configure terminal`
    - `ssh disable`
    - `copy running-config startup-config`

We have no evidence of any other individual products being vulnerable to this but as a precaution we strongly recommend adhering to best practices by not exposing SSH or any interfaces to the public internet. Further updates will be provided as our investigation progresses.