AIRASHI Botnet Attacks

Cambium Networks is aware of reports of the AIRASHI botnet targeting cnPilot products. We are currently investigating this issue.

Our preliminary analysis indicates that cnPilot R series routers with weak or default passwords are the target. We strongly recommend that customers

- Update device firmware to the latest recommended version available in cnMaestro or here
- Change default or weak passwords for all three user accounts (admin, normal and basic)
- Disable remote web and remote ssh access, and disable telnet if enabled

The passwords and remote web access setting can be changed in cnMaestro under AP Group -> Management. Remote ssh and telnet are disabled in cnMaestro, and these settings cannot be directly changed by the user. If necessary, these two settings can be disabled by adding the following user defined overrides as described here.

```
DBID_LAN_LOGIN_ONLY=1

SSH_SERVER_REMOTE_ENABLE=0
```

Instructions on changing these settings from the device web UI are available here.

We have no evidence of cnPilot E series or any other Cambium products being affected. Further updates will be provided as our investigation progresses.