Connect Wi-Fi Thermostat Security Features

Rev. 1/8/2018

Carrier is committed to the security of our products. As such, we have designed the Connect Stat and associated mobile application and web site with security features that help protect end users' building networks from unauthorized access. These features include:

- The Connect Wi-Fi thermostat supports WEP, WPA, and WPA2 authentication.
- Wi-Fi connectivity supports 802.11 a/b/g/n standards on 2.4 GHz networks.
- All data is encrypted in the database and in transit (HTTPS & UDP) using AES-256 encryption and TLS 1.0-1.2.
- Secure Wi-Fi connections are not interrupted during Over-the-Air (OTA) upgrades.
- Security updates, if necessary, are managed as OTA pushes and do not require manual interface by a local user.
- The web portal does not support user-supplied redirects. This helps prevent invalid redirects or web site forwards.
- To help prevent cross-site request forgery, all requests require an authorization header. This authorization header only responds to a direct XMLHttpRequest and cannot be spoofed by a form, URL, or any other means. External XMLHttpRequests are blocked by the web portal's server.
- User access to the Ayla Agent (cloud-based service) and the Connect Stat mobile app are password protected. These passwords are user generated and no defaults exist. The Ayla agent uses certificate based authentication when communicating with the Connect Stat. All passwords are salted and hashed.
- Wi-Fi connectivity can be disabled through the local user interface. This will disable access to the stat when using the app and web site. Several key functions will also become disabled (scheduling changes, remote alarm notification).

One of the more common ways security measures are circumvented is the "remember me" functionality built into many web browsers and mobile apps. Utilizing this feature may create a "long lived session" where refresh tokens are not expired until the user manually logs out. This could allow unauthorized access to the account email and/or passwords. To help prevent this risk, we recommend not using the "remember me" function.

If you believe you have discovered a vulnerability or would like additional details about our commitment to security, please use the following link: vulnerability reporting site (https://www.carrier.com/commercial/en/us/i-vu/security)