ENCELIUM Networked Light Management System

Security Statement

Encelium views security as paramount to any light management solution. Accordingly, Encelium employs a multi-tiered approach to identify and manage security risks within the Encelium X Networked Light Management System.

The following is the multi-faceted approach Encelium uses to manage security within our networked solutions.

1. **Physical Security**
    a. Access to the Encelium X Manager requires access to the internal Ethernet or physical access to the unit.
    b. The only connection to the Encelium X Manager is via Ethernet; there is no Wi-Fi connection. Ethernet access is limited to Encelium X System services safeguarded by a firewall. To further enhance security, the Encelium X System can be segmented from the customer network (via VLAN for example).

2. **Customer Security**
    a. Access rights and user credentials can be configured by end user
    b. Multiple levels of roles-based access (Administrator, Operator, Monitor Only)
    c. Customer provides an additional layer of access security to the Encelium X System by having strong corporate network access credentials in place and limiting devices that can access those networks.
    d. Encelium advises customers to follow their corporate best practices in selecting the installation method that best meets their building and application requirements.

3. **Wireless Device Communication Security**
    a. While acting as the Zigbee® coordinator, the Encelium X Wireless Manager (“WM”) uses whitelisting to allow ONLY trusted devices to join the Encelium X Network. Additionally, the WM is hardened against common attacks such as “replay”, “injection” and “denial of service”.

b. Security between devices is further enhanced using the following techniques:

i. Periodic changes to the Network Key via 128-bit transport key that is shared by all devices in the Encelium X System to protect management and control communications.

ii. Enhanced non-public Link Key is used to negotiate the Transport Encryption Key.

iii. 128-bit AES Encryption is applied to the Zigbee Network Layer ensuring the integrity of all transmitted data.

4. Controller-to-Controller Communication Security

a. Inter-Manager communication uses TLS 1.2 encryption.

b. Client-to-controller uses HTTPS.

5. Network Segmentation Security

a. Wireless

i. Each Encelium X WM on the lighting network uses a unique encryption key.

ii. The wireless light management network is containerized, and each WM is individually secured.

iii. Wireless segmentation is done at the wireless network, not the Ethernet network.

b. Wired

i. The wired Fieldbus (lighting specific protocol) via the Encelium X Manager is not capable of carrying other protocols or malicious payloads.

ii. The wired Fieldbus does not have access to the corporate Ethernet network.

6. OTA Update Security

a. End-to-end encryption is used during firmware and software updates.

- # # # -