iManifold® PULSE! ™

Device Security Considerations

North Park Innovations Group, Inc.
P.O. Box 900; 6442 Route 242 East
Ellicottville, NY 14731
716-699-2031
www.imanifold.com

Overview

North Park Innovations Group, Inc. (NPI) is the manufacturer of the iManifold® Pulse™ (Pulse) devices. Pulse devices are assembled at our main production facility in Ellicottville, New York.

The purpose of this paper is to present a set of security guidelines and best practices that our customers can use in order to secure their iManifold Pulse devices on their internal networks.

It focuses on defining the pre-existing security features of the Pulse device as well as recommendations and guidance for deploying them.

Pulse devices are meant to operate continuously unattended and not subject to the security of frequent, direct human observation. Our guidance is to isolate these devices from your internal network via standard security practices which are outlined later in this document.

Should you have any questions about this paper, or the Pulse devices, please contact us.

North Park Innovations Group, Inc.
P.O. Box 900; 6442 Route 242 East
Ellicottville NY 14731
716-699-2031
www.imanifold.com

System and Device Security

Tamper Resistance

The Pulse devices are protected by a **hard-plastic enclosure** and have optional **security screws** to discourage tampering with the internal mechanisms of the device, if necessary, in your installation location.

Additionally, the Pulse devices can be mounted inside HVAC enclosures to add additional physical protection to access the devices in the field.

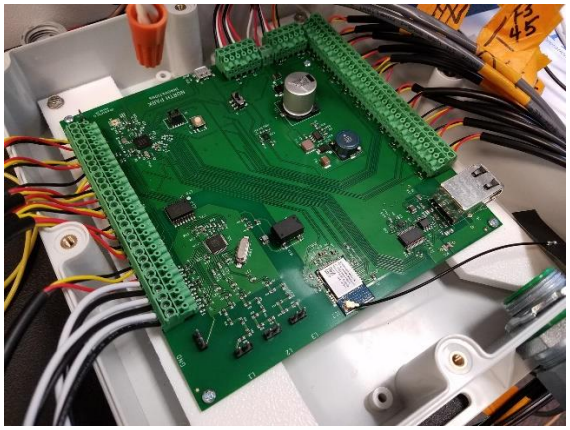
There is no capability to login to the device via direct physical connection (i.e. monitoring or network cables) either at rest or upon startup or reset. No firmware can be uploaded or updated except that which matches each device's public / private key encryption algorithm.

Firmware and Patch Management

Firmware and software patching of Pulse devices can only be accomplished by an authorized technician, connecting to the device using the mobile application over Bluetooth and updating the device using the public / private key encryption system.

System and Device Security Continued

Dynamic Testing



Each Pulse device's circuit board is tested prior to delivery for Bluetooth, ethernet and WIFI functionality along with general manufacturing quality and internal standards.

Each device's firmware is uploaded by NPI during the manufacturing process and that code is accessible only to NPI. A multi- step process is implemented to connect, upload and test the firmware on each device.

Data Protection Upon Disposal

No proprietary customer data is stored on the Pulse devices at any time. The only data stored on the device is basic configuration information that is kept in the flash memory of each unit.

Device Broadcasting

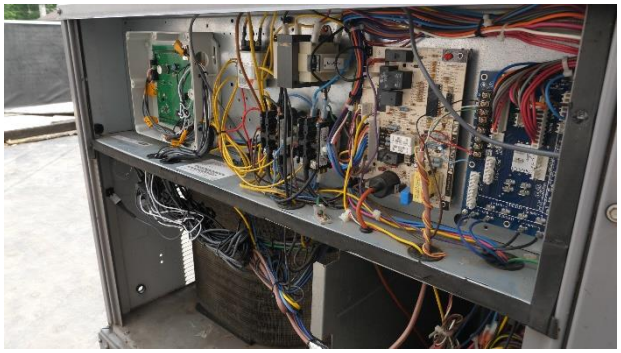
No proprietary or customer identifiable information is broadcast by the Pulse devices during the course of their normal operation.

Independent Testing and Certification

North Park Innovations Group’s iManifold Pulse manufacturing processes have been found to comply with the U.S. Listing/Certification requirements and have been approved by F2 Labs (www.f2labs.com) and an A2LA accredited testing laboratory (SGS) who is an OSHA recognized Nationally Recognized Test Lab (NRTL).

Customer Network Security

Authentication



Pulse devices arrive at customer locations with no pre-loaded customer information or access ability by anyone other than the authorized technician.

Authorized technicians set-up the device using specific credentials personalized to that device and the configuration of a unique security token is created to allow the device to begin to communicate to the back-end monitoring system.

There is no "back-door" or debug access to the devices and no ability to connect to the device prior to the generation of the security token by the authorized technician.

Encryption and Protocols

Pulse devices communicate over standard network communication protocols including TCP-IP over Ethernet and Wi-Fi as well as Bluetooth.

Communication between the Pulse devices and the backend monitoring systems is encrypted using HTTPS/ TLS.

Device Bandwidth Minimization

Pulse devices are programmatically limited to sending data back to the monitoring platform at intervals of once per minute. This is a designed and controlled transmission schedule requiring a minimum amount of bandwidth. By programming the transmission intervals, Pulse devices cannot be used in any type of DDoS attack.

Customer Network Security Continued

Network Segmentation Best Practices

We recommend that Pulse devices be separated from normal internal network traffic into their own security zone and VLAN on our customer's internal networks.

By creating separate security zones and VLANs Pulse devices can be segmented from the normal internal private network allowing specific security policies to be enforced on that zone ensuring that all traffic related to the Pulse device does not interact with other internal networks.

Our recommended best practices for network segmentation of the Pulse device includes the following:

- **Create a separate or add to an existing Controlled Security Zone on your firewall**
- **Create a separate VLAN for Pulse devices and assign it to the Controlled Security Zone**
- **Issue and assign an internal static IP address for each Pulse device**
- **Set Firewall Rules to allow outbound traffic from the Pulse VLAN to the Internet only.**
- **Set Outbound traffic over Internet to the prescribed Pulse Monitoring System external IP Address Range (Optional)**