September 3, 2013

Dear i-Vu® Pro v6.0 Owner:

Given the heightened security awareness in all aspects of our society, it is not surprising that customers are concerned about whether or not the i-Vu Pro application poses a security risk to their building network. While there is no such thing as a system that is absolutely invulnerable to hackers, the inherent design and security aspects of the i-Vu Pro application make it extremely unlikely that anyone could gain unauthorized access to the building network through the i-Vu Open system. There are several key reasons why i-Vu Pro does not pose a security risk:

- i-Vu Pro web server engine:
    - The i-Vu Pro application uses its own, built-in web server engine. It does not utilize the Microsoft IIS web server. The built-in web server is only used by the i-Vu Pro system and is not shared by any other system on the network.
    - The web server renders only i-Vu Pro pages. It cannot be used as a general-purpose web server to render pages from other systems on the building network.
    - All database queries use a single internal interface that protects against common SQL injection attacks. As of v6.0, this includes Write to Database alarm actions.
    - As of v6.0, the i-Vu Pro Server application no longer uses Java Applets or Java Web Start which have been the source of Java vulnerabilities to desktop computers.
- I-Vu Pro communications:
    - There are 2 categories of protocols and ports that the i-Vu Pro application uses: **Client /Server** and **Server/i-Vu router**. **Client/Server** is the communications between the end user's computer (whether remote or local) and the i-Vu server. **Server/i-Vu router** is the communications between the i-Vu Server application and the network interface (specifically with an i-Vu router). If a firewall exists between the Client and Server or the Server and Device Manager path, special attention must be paid to the list below. If a firewall exists between the Client and Server or the Server and i-Vu router, the ports in the following table must be open to enable communication.

A list of ALL the protocols, ports and reason for use is as follows:

Server Ports (Listening Ports)

Port	Transfer	Protocol/User	Use
80	TCP	http (Web Server)	Client/Server
443	TCP	https (Web Server)	Client/Server
47806	TCP	Alarm Pop-up Client	Client/Server
47808	UDP	Bacnet/IP	Server/i-Vu router
47808	TCP	Diagnostic Telnet	Client/Server
47812	UDP	Pro/IP	Server/i-Vu CCN router
50005 - 50008	UDP	Firmware Pro/IP	Server/i-Vu CCN router

- You can edit the default http and https ports in SiteBuilder and the default **Alarm Pop-up** port in the i-Vu interface (**System Options** tree > **System Settings** > **General** tab > **Alarms**).
- The i-Vu Pro Server application does not require open ports for traditional Telnet, FTP, Windows file sharing, or other applications that can increase the vulnerability of the system. The Diagnostic Telnet port listed above is a password-protected text-only UI that is limited to i-Vu functions. This is ONLY used for Tech Support purposes and should be firewalled.
- Built-in support for Secure Socket Layer (SSL) communications provides 128-bit encryption for all communications to ensure unauthorized 'eavesdroppers' cannot obtain passwords. If needed, you can increase the encryption level to 256-bit. (See "Network Security" in i-Vu Pro Help for information on configuring SSL). All network traffic between the i-Vu Pro Server application and the browser can be encrypted using a locally created certificate. The i-Vu Pro software suite offers tools to recreate these certificates at any time, export to a third-party Certificate Authority (CA), and re-import the signed certificate.
- An i-Vu Pro server with two NICs can provide additional security and easier system diagnostics. One NIC is dedicated to web page traffic, and the other to unencrypted BACnet traffic to field controllers. This separation of physical networks is the recommended best practice for building security. In this configuration, it is impossible for BACnet traffic to cross between the two networks
- The i-Vu Pro web server is “locked down” and only renders i-Vu® Pro pages. It cannot be used as a general-purpose web server to render pages from other systems on the building network.

- Operator access to the i-Vu Pro Server application:
  - The i-Vu Pro application offers an extremely “fine grained” password security control, allowing operator privileges to be custom-tailored for each operator, providing no more access than required.
  - Access to the i-Vu Pro Server application can be restricted based on geographic assignment of operator privileges. For example, this allows persons with the same operator privileges access to different geographic areas of the system (i.e. two different rooms, floors, or buildings).
  - The i-Vu Pro audit log provides a detailed list of all operator actions and can be searched by operator name, date, and geography.

- In a 21CFR Part 11 Pharmaceutical/Biotech validated facility, the i-Vu Pro Server application can require an operator to record the reason for a change to operating conditions before accepting the change.

- As of v6.0, operator passwords are “salted” and “hashed” using SHA512 and therefore cannot be reversed-engineered and are not exposed if the i-Vu Pro database is compromised.
- As of v6.0, passwords that the i-Vu Pro Server application uses to access other systems use AES-128 bit encryption. This includes database passwords.
- In addition to the inherent protection listed above, i-Vu Pro is compatible with external security provisions, such as firewalls and Virtual Private Networks (VPNs), that the customer’s IT staff may wish to use. These systems can limit access to specific computer IDs and provide an additional layer of login/password protection, as well as offering alternative encryption schemes.

If you have additional questions, please feel free to contact your local Carrier office.

Sincerely,

Carrier Systems Support