May 1, 2014
Rev. 1

Dear i-Vu® Standard/Plus 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 Standard or Plus 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 application make it extremely unlikely that anyone could gain unauthorized access to the building network through the i-Vu web server. There are several key reasons why i-Vu does not pose a security risk:

- i-Vu Standard or Plus web server engine:
  - The i-Vu 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 system and is not shared by any other system on the network.
  - The i-Vu web server is “locked down” and only renders i-Vu 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.
  - The i-Vu web server runs a custom, streamlined version of the Linux operating system. The i-Vu database is restricted to internal connections only and cannot be accessed externally.
  - As of v6.0, the i-Vu application no longer uses Java Applets or Java Web Start which have been the source of Java vulnerabilities to desktop computers.

- i-Vu Standard or Plus communications

- The protocols and ports that are used by the i-Vu application can be partitioned into 3 categories: Client /Server, Basic Network, and Server/i-Vu router. Client/Server is the path between the end user’s computer (whether remote or local) and the i-Vu web server. Server/i-Vu router is the path between the i-Vu web server and a network interface (specifically with an i-Vu router). Basic Network is the path between the i-Vu web server and external network services, such as DNS or NTP. 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.

The following lists ALL the protocols, ports, and reasons to use them:

Server Ports (Listening Ports)

Port	Transfer	Protocol/User	Use
68	UDP	DHCP Client daemon	Basic Network
80	TCP	http (Web Server)	Client/Server
123	UDP	NTP (Network Time Protocol)	Basic Network
137	UDP	nmbd (netbios/tcp requests)	Basic Network
138	UDP	nmbd (netbios/tcp responses)	Basic Network
443	TCP	https (Web Server)	Client/Server
8080	TCP	http (Management Tool)	Client/Server
47806	TCP	Alarm Pop-up Client	Client/Server
47808	UDP	Bacnet/IP	Server/Gateway
47808	TCP	Diagnostic Telnet	Client/Server
47812	UDP	CCN/IP	Server/i-Vu CCN router
50005-50008	UDP	Firmware CCN/IP	Server/i-Vu CCN router

- You can view and define HTTP and HTTPS ports in the Management Tool. You can also define the the Alarm Pop-up port (**System Options** > **General** > **Alarms**).

- The i-Vu Management Tool uses the Ruby WEBrick 1.3.1 server on port 8080. The i-Vu server does not open ports for traditional Telnet, FTP, Windows file sharing, or other applications that 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 otherwise.

- Operator access to the i-Vu application

  - i-Vu offers an extremely “fine grained” password security control, allowing operator privileges to be custom-tailored for each operator, providing no more access than required.

  - The i-Vu audit log provides a detailed list of all operator actions and can be searched by operator name, date, and geography.

  - The i-Vu application offers built-in support for Secure Socket Layer (SSL) communications, providing up to 256-bit encryption for all communications, to ensure that unauthorized “eavesdroppers” cannot obtain private information.

  - The i-Vu application supports SHA 512-bit hashed login password security, further enhanced by the use of a salting algorithm to prevent password exposure.

- The i-Vu system stores email, and remote system access passwords using AES 128-bit encryption.

- In addition to the inherent protection listed above, i-Vu 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