September 4, 2013

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:

- 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.
- 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.
- The HTTP, HTTPS, and Alarm Pop-up Utility ports are the only user-configurable ports in the system. They can be viewed and/or modified using the i-Vu Management Tool.
- The i-Vu Management Tool uses the Ruby WEBrick 1.3.1 server on port 8080. The i-Vu web server does not open ports for traditional Telnet, FTP, Windows file sharing, or other applications that increase the vulnerability of the system.
- The i-Vu 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.
- 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, the i-Vu system 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.

For a detailed list of ports and protocols that are used by the i-Vu web server, or if you have additional questions, please feel free to contact your local Carrier office.

Sincerely,

Carrier Systems Support