Carrier
A United Technologies Company

August 1, 2008

Dear i-Vu CCN 4.2 Standard/PLUS Owner:

Given the heightened security awareness in all aspects of our society, it is not surprising that customers are concerned about whether or not i-Vu CCN 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 i-Vu CCN make it extremely unlikely that anyone could gain unauthorized access to the building network through the i-Vu CCN web server. There are several key reasons why i-Vu CCN does not pose a security risk:

- i-Vu CCN uses its own, built-in web server engine (Tomcat). It does not utilize the Microsoft IIS web server, which is a favorite and well-known target for hackers. This web server is only used by the i-Vu CCN system and is not shared by any other system on the network.
- The i-Vu CCN web server runs a custom, streamlined version of the Linux operating system. The i-Vu CCN database is restricted to internal connections only and cannot be accessed externally.
- The protocols and ports that are used by i-Vu can be partitioned into two categories: Client / Server and Server/Gateway. Client/Server is defined as the path between the end user's PC (whether remote or local) and the i-Vu CCN web server. Server/Gateway is defined as the path between the i-Vu CCN web server and a network interface (specifically with the i-Vu Link, i-Vu CCN Router, and CCN Ethernet Converter). If a firewall exists between either component of the Client/Server or Server/Device Manager path, special attention must be paid to the list below.

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

Server Ports (Listening Ports)

Port	Transfer	Protocol/User	Use
68	UDP	DHCP Client daemon	Basic Network
80	TCP	http (Web Server)	Client/Server
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/Gateway
50005 - 50008	UDP	Firmware CCN/IP	Server/Gateway

- HTTP and HTTPS ports are user-viewable/definable via the Management Tool. The alarm pop-up port is user-definable via System Options -> General -> Alarm Pop-up (at the bottom of the screen). All other ports are NOT configurable.

The i-Vu CCN Management Tool uses the Ruby WEBrick 1.3.1 server on port 8080. The i-Vu CCN 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.

- The i-Vu CCN web server is "locked down" and will only render i-Vu CCN pages. It cannot be used as a general-purpose web server to render pages from other systems on the building network.
- i-Vu CCN offers an extremely "fine grained" password security control, allowing operator privileges to be custom tailored for each operator, providing no more access than is required.
- i-Vu CCN offers built-in support for Secure Socket Layer (SSL) communications, providing 128-bit encryption for all communications to ensure that unauthorized "eavesdroppers" cannot obtain passwords.

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