i-Vu Standard/Plus v7.0 Security

Rev. 7/2/2018

The i-Vu® Standard/Plus application provides a very high level of security to protect against unauthorized access. This memorandum briefly outlines design, security, configuration, and implementation aspects of your i-Vu Building Automation System server application.

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

- i-Vu source code is subjected to source code analysis and independent third-party penetration testing as part of our software development lifecycle process.

- All third-party libraries are scanned for known vulnerabilities.

- i-Vu® Standard/Plus web server engine:
    - The i-Vu server application uses its own built-in web server engine based on a locked-down version of Apache Tomcat. This greatly reduces the chance of an undiscovered Apache Tomcat vulnerability.
    - 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 server application does NOT use Microsoft's IIS web server.
    - The web server renders only 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 server application no longer uses Java® Applets or Java Web Start which have been the source of Java vulnerabilities to desktop computers. While the i-Vu server application no longer uses Applets or Web Start, we do recommend that customers keep their Java Runtime Environment up to date at all times.

  - i-Vu Plus allows only add-on applications provided and signed by Carrier. i-Vu Standard does not allow add-on applications.

- i-Vu® Standard/Plus communications:
  - The i-Vu server application uses the ports and protocols listed in the following table. In the **Use** column, **Client/Server** is communication between the end user's computer and the i-Vu web server. **Server/i-Vu router** is communications between the i-Vu web server and the Ethernet network interface on a Carrier IP controller. **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, you will need to open the following ports to enable communication.

Port	Transfer	Protocol/User	Use
68	UDP	DHCP Client daemon	Basic Network
80 (default)	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 (default)	TCP	https (Web server)	Client/Server
8080	TCP	http (Management Tool)	Client/Server
47806 (default)	TCP	Alarm Notification Client	Client/Server
47808	UDP	BACnet/IP	Server/i-Vu router
47808	TCP	Diagnostic Telnet *	Client/Server
47812	UDP	CCN/IP	i-Vu CCN router/Server
50005	UDP	Firmware CCN/IP	Server/i-Vu CCN router

* This functionality is off by default. You can start it using the `telnetd` console command.

  - You can edit the default Alarm Notification Client port in the i-Vu interface (System Options > General tab > Alarms).
  - You can edit the default http and https ports in the Management Tool.
  - The i-Vu Management Tool uses the Ruby WEBrick 1.3.1 server on port 8080.
  - The i-Vu server application does not require open ports for standard Telnet, FTP, Windows file sharing, or other applications that can increase the vulnerability of the system. The **Diagnostic Telnet** protocol used on port 47808 is a password-protected plain text only user interface that is limited to i-Vu server application functions. This functionality is ONLY used for Tech Support purposes and should be firewalled. It is turned off by default. You can start it using the `telnetd` console command.

  - 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 Help for information on configuring SSL.) All network traffic between the i-Vu server application and the browser can be encrypted using a locally created certificate.
  - The i-Vu server application is compatible with standard external security provisions such as firewalls and Virtual Private Networks (VPNs). VPNs can limit access to specific computer IDs, provide an additional layer of login/password protection, and offer alternative encryption schemes.
  - The 6-02 and later drivers support BACnet whitelist functionality. You can restrict traffic to all private IP addresses and/or a list of specific IP addresses. This can also be used on an isolated network to restrict traffic to only designated BACnet devices and workstation(s) to ensure no other IP devices can tamper with BACnet controllers.

- Operator access to the i-Vu® Standard/Plus application:
  - i-Vu password security allows operator access based on roles set by the administrator. The advanced security policy provides further security through password character/expiration requirements and user lockouts.
  - The i-Vu audit log provides a detailed list of all operator actions and can be searched by operator name, date, and geography.
  - 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 database is compromised. This also means that Carrier cannot help recover lost passwords.
  - As of v6.0, passwords that the i-Vu server application uses to access other systems use AES-128 bit encryption.

- As of v7.0, all patches to the i-Vu software are signed for authentication and to prevent tampering.

- See our *Security Best Practices* document for additional best practices and a security checklist.