Customer Service Bulletin

Products:	**Welch Allyn ELI** 150c, BUR 150c, **Welch Allyn ELI** 250c, **Welch Allyn ELI** 280, and **Welch Allyn ELI** 380 Resting Electrocardiographs	**Date:**	24-JUN-2022
Subject:	Security Vulnerability of Improper Access Control		
HW Version(s) Affected:	WLAN – 9910-023-06 (B&B)	**SW Version(s) Affected:**	N/A
Serial Numbers Affected:	N/A	**Lot or Date Code Affected:**	N/A

Disposition:	Reactive Service Use
Distribution:	☒ Customer Care ☒ Product Service ☒ Field Service ☒ ASPs ☒ Distributors ☒ Customers ☐ Company Confidential
Training Required:	☒ Yes ☐ No
Summary:	A cyber security risk was identified in the **Welch Allyn ELI** 280 Resting Electrocardiograph. The risk applies to the B&B WLAN module (PN-9910-023-06). The provisioned WLAN module WLNN-AN-MR551 which is a customized version of the WLN-AN-DP551 Airborne embedded dual-band wireless module used in the **Welch Allyn ELI** 280 device, **Welch Allyn ELI** 380 (older versions) device, and **Welch Allyn ELI** 150c device contains default configurations that left several ports and services open, which allow potential access to the radio by unauthorized users. Specifically, port 21 FTP service, port 22 SSH (Secure Shell Connection) and port 23 Telnet service are enabled by the default configuration settings. No known public exploits specifically target these vulnerabilities. These vulnerabilities have high attack complexity.

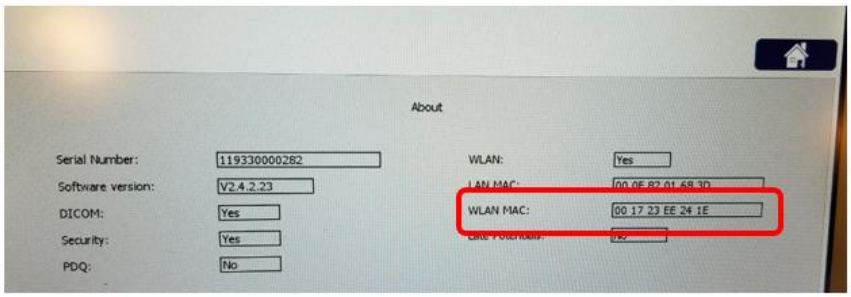
Mitigation:

Hillrom is releasing software updates for all impacted devices to address these vulnerabilities.

ELI380 units with the LAIRD/NEWMAR WLAN radio installed are not impacted by these vulnerabilities (regardless of software version).

The WLAN type can be identified as shown below:

The WLAN MAC address is located under the SETTINGS function of the cardiograph, and will appear as shown below.



The MAC address contains 12 characters, where the first 6 characters are used to determine the model of the WLAN module installed. The remaining 6 digits will change with each device.

B&B module = 00 0B 28 xx xx xx

Laird module = 00 17 23 xx xx xx

For units with the B&B WLAN radio installed, the following mitigations would apply:

New product versions that mitigate these vulnerabilities are available as follows:

- **Welch Allyn ELI** 380 Resting Electrocardiograph: available by Q4 2023
- **Welch Allyn ELI** 280/BUR280/MLBUR 280 Resting Electrocardiograph: Software version 2.4.1, available June 2022
- **Welch Allyn ELI** 150c/BUR 150c/MLBUR 150c Resting Electrocardiograph: available by Q4 2023

Hillrom recommends users upgrade to the latest product versions. Customers should contact Technical Support for assistance.

The following actions can be taken by facility IT resources today to reduce risk associated with this vulnerability.

- Apply proper network and physical security controls.
- Disabling FTP and Telnet on the facility network.
- Ensure a unique encryption key is configured for ELI Link and cardiographs, per instructions in the product user manual.
- Locate control system networks and remote devices behind firewalls and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that a VPN is only as secure as the connected devices.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their finding to CISA or tracking and correlation against other incidents.

CISA Contact Information:

- Phone - +1-888-282-0870
- Email – CISAservicedesk@cisa.dhs.gov

Resolution: This issue has been documented into our feedback system (B104662, B104650, B104660) for correction in a future software release.

Version	Sec, Pg, Para Changed	Change Made	Date Version Created	Version Created By (initials)
A	N/A	Initial Release	16-JUN-2022	SLB
B	Mitigation	Added detail to determine if **Welch Allyn ELI** 380 device affected	24-JUN-2022	SLB