ACTIVITY ALERT

Industrial Control Systems Advisory

ICSMA-22-167-01 NUMBER

June 16, 2022 DATE

ICSMA-22-167-01 Hillrom Medical Device Management

1 EXECUTIVE SUMMARY

- **CVSS v3 7.7**
- **ATTENTION**: Exploitable remotely/low attack complexity
- **Vendor**: Hillrom Medical. Welch Allyn and ELI are registered trademarks of Baxter International, Inc., or its subsidiaries.
- **Equipment**: Welch Allyn medical devices
- **Vulnerabilities**: Use of Hard-coded Password, Improper Access Control

2 RISK EVALUATION

Successful exploitation of these vulnerabilities could allow an attacker to compromise software security by executing commands, gaining privileges, reading sensitive information, evading detection, etc.

3 TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following Hillrom products, are affected:

- Welch Allyn ELI 380 Resting Electrocardiograph: Versions 2.6.0 and prior
- Welch Allyn ELI 280/BUR280/MLBUR 280 Resting Electrocardiograph: Versions 2.3.1 and prior
- Welch Allyn ELI 250c/BUR 250c Resting Electrocardiograph: Versions 2.1.2 and prior
- Welch Allyn ELI 150c/BUR 150c/MLBUR 150c Resting Electrocardiograph: Versions 2.2.0 and prior

3.2 VULNERABILITY OVERVIEW

3.2.1 USE OF HARD-CODED PASSWORD CWE-259

The affected products contain hard-coded (unchangeable) passwords used for inbound authentication or outbound communication to external components.

CVE-2022-26388 has been assigned to this vulnerability. A CVSS v3 base score of 6.4 has been calculated; the CVSS vector string is (AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L).

3.2.2 IMPROPER ACCESS CONTROL CWE-284

The software does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

CVE-2022-26389 has been assigned to this vulnerability. A CVSS v3 base score of 7.7 has been calculated; the CVSS vector string is (AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:H).

3.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Healthcare and Public Health
- **COUNTRIES/AREAS DEPLOYED:** Worldwide
- **COMPANY HEADQUARTERS LOCATION:** United States

3.4 RESEARCHER

An anonymous user reported these vulnerabilities to Hillrom.

4 MITIGATIONS

Hillrom has released software updates for all impacted devices to address these vulnerabilities. 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: available May 2022
- Welch Allyn ELI 150c/BUR 150c/MLBUR 150c Resting Electrocardiograph: available by Q4 2023

Hillrom recommends users upgrade to the latest product versions. Information on how to update these products can be found on the Hillrom disclosure page.

Hillrom recommends the following workarounds to help reduce risk:

- Apply proper network and physical security controls.
- Ensure a unique encryption key is configured for ELI Link and Cardiograph.
- Where possible, use a firewall to prevent communication on Port 21 FTP service, Port 22 SSH (Secure Shell Connection), and Port 23 Telnet service.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on cisa.gov/ics. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on cisa.gov/ics in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

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

No known public exploits specifically target these vulnerabilities.

5 CONTACT INFORMATION

Recipients of this report are encouraged to contribute any additional information they may have related to this threat. Include the reference number in the subject line of all email correspondence. For any questions related to this report, please contact CISA:

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

6 FEEDBACK

CISA continuously strives to improve its products and services. You can help by answering a few short questions about this product at https://www.cisa.gov/uscert/forms/feedback