ACTIVITY ALERT

ICSMA-21-343-01 NUMBER

Industrial Control Systems Advisory

December 9, 2021 DATE

ICSMA-21-343-01 Hillrom Welch Allyn Cardio Products

1 EXECUTIVE SUMMARY

- **CVSS v3 8.1**
- **ATTENTION**: Exploitable remotely
- **Vendor**: Hillrom
- **Equipment**: Welch Allyn Cardio Products
- **Vulnerability**: Authentication Bypass Using an Alternate Path or Channel

2 RISK EVALUATION

Successful exploitation of this vulnerability could allow an attacker to access privileged accounts.

3 TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following Hillrom cardiology products, when configured to use single sign-on (SSO), are affected:

- Welch Allyn Q-Stress Cardiac Stress Testing System: Versions 6.0.0 through 6.3.1
- Welch Allyn X-Scribe Cardiac Stress Testing System: Versions 5.01 through 6.3.1
- Welch Allyn Diagnostic Cardiology Suite: Version 2.1.0
- Welch Allyn Vision Express: Versions 6.1.0 through 6.4.0
- Welch Allyn H-Scribe Holter Analysis System: Versions 5.01 through 6.4.0
- Welch Allyn R-Scribe Resting ECG System: Versions 5.01 through 7.0.0
- Welch Allyn Connex Cardio: Versions 1.0.0 through 1.1.1

3.2 VULNERABILITY OVERVIEW

3.2.1 AUTHENTICATION BYPASS USING AN ALTERNATE PATH OR CHANNEL CWE-288

The impacted products, when configured to use SSO, are affected by an improper authentication vulnerability. This vulnerability allows the application to accept manual entry of any active directory (AD) account provisioned in the application without supplying a password, resulting in access to the application as the supplied AD account, with all associated privileges.

CVE-2021-43935 has been assigned to this vulnerability. A CVSS v3 base score of 8.1 has been calculated; the CVSS vector string is (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).

3.3 BACKGROUND

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

3.4 RESEARCHER

Hillrom reported this vulnerability to CISA.

4 MITIGATIONS

Hillrom plans to release software updates to address this vulnerability in their next software release.

In the interim, Hillrom recommends the following workaround and mitigation to reduce the risk:

- Disable the SSO feature in the respective Modality Manager Configuration settings. Please refer to the instructions for use (IFU) and/or service manual for instructions on how to disable SSO.

Hillrom recommends users to upgrade to the latest versions of their products once they've been made available. Information on how to update these products to their new versions can be found on the Hillrom disclosure page.

Hillrom recommends the following additional workarounds to help reduce risk:

- Apply proper network and physical security controls.
- Apply authentication for server access.

CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability. Specifically, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure they are not accessible from the Internet.
- 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 VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its connected devices.

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 us-cert.cisa.gov. 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 us-cert.cisa.gov 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 this vulnerability. This vulnerability has a high attack complexity.

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://us-cert.cisa.gov/forms/feedback