ACTIVITY ALERT

Industrial Control Systems Advisory

ICSA-21-152-01 NUMBER

November 17, 2022 DATE

ICSMA-21-152-01 Hillrom Medical Device Management (Update C)

1 EXECUTIVE SUMMARY

- **CVSS v3 5.9**
- **ATTENTION**: Exploitable remotely
- **Vendor**: Hillrom
- **Equipment**: Welch Allyn medical device management tools
- **Vulnerabilities**: Out-of-Bounds Write, Out-of-Bounds Read

2 UPDATE INFORMATION

This updated advisory is a follow-up to the original advisory titled ICSA-21-152-01 Hillrom Medical Device Management (Update B) that was published September 8, 2022, to the ICS webpage at www.cisa.gov/uscert.

3 RISK EVALUATION

Successful exploitation of these vulnerabilities could allow an attacker to cause memory corruption and remotely execute arbitrary code.

4 TECHNICAL DETAILS

4.1 AFFECTED PRODUCTS

The following Hillrom products, are affected:

Welch Allyn Service Tool: versions prior to v1.10

Welch Allyn Connex Device Integration Suite – Network Connectivity Engine (NCE): versions prior to v5.3

Welch Allyn Software Development Kit (SDK): versions prior to v3.2

Welch Allyn Connex Central Station (CS): versions prior to v1.8.4 Service Pack 01

Welch Allyn Service Monitor: versions prior to v1.7.0.0

Welch Allyn Connex Vital Signs Monitor (CVSM): versions prior to v2.43.02

Welch Allyn Connex Integrated Wall System (CIWS): versions prior to v2.43.02

DISCLAIMER: This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as TLP:WHITE: Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to. For more information on the Traffic Light Protocol, see https://us-cert.cisa.gov/tlp

Welch Allyn Connex Spot Monitor (CSM): versions prior to v1.52
Welch Allyn Spot Vital Signs 4400 Device (Spot 4400) / Welch Allyn Spot 4400 Vital Signs Extended Care Device: versions prior to v1.11.00

4.2 VULNERABILITY OVERVIEW

4.2.1 OUT-OF-BOUNDS WRITE CWE-787

The affected product is vulnerable to an out-of-bounds write, which may result in corruption of data or code execution.

CVE-2021-27410 has been assigned to this vulnerability. A CVSS v3 base score of 5.9 has been calculated; the CVSS vector string is (AV:A/AC:H/PR:L/UI:N/S:U/C:L/I:H/A:L).

4.2.2 OUT-OF-BOUNDS READ CWE-125

The affected product is vulnerable to an out-of-bounds read, which can cause information leakage leading to arbitrary code execution if chained to the out-of-bounds write vulnerability.

CVE-2021-27408 has been assigned to this vulnerability. A CVSS v3 base score of 5.9 has been calculated; the CVSS vector string is (AV:A/AC:H/PR:L/UI:N/S:U/C:L/I:H/A:L).

4.3 BACKGROUND

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

4.4 RESEARCHER:

Itamar Cohen-Matalon of Medigate Reserach Labs reported these vulnerabilities to Hillrom.

5 MITIGATIONS

Hillrom has released software updates for all impacted devices to address these vulnerabilities. New versions of the products that mitigate the vulnerabilities are available as follows:

Welch Allyn Service Tool: v1.10

Welch Allyn Software Development Kit (SDK): v3.2

--------- Begin Update C Part 1 of 1 ---------

Welch Allyn Connex Central Station (CS): v1.8.4 Service Pack 01 (released November 2022)

--------- End Update C Part 1 of 1 ---------

Welch Allyn Connex Device Integration Suite - Network Connectivity Engine (NCE): v5.3 (released September 2021)

Welch Allyn Spot Vital Signs 4400 Device (Spot 4400) / Welch Allyn Spot 4400 Vital Signs Extended Care Device: v1.11.00 (released October 2021)

Welch Allyn Service Monitor: v1.7.0.0

Welch Allyn Connex Vital Signs Monitor (CVSM): v2.43.02

Welch Allyn Connex Integrated Wall System (CIWS): v2.43.02

Welch Allyn Connex Spot Monitor (CSM): v1.52

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

Hillrom recommends the following workarounds to help reduce risk:

Apply proper network and physical security controls.

Apply authentication for server access.

Apply data execution prevention (DEP) where applicable to help prevent shellcode from running. Address space layout randomization (ASLR) is built into standard Windows and Linux distributions.

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

- 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 VPN is only as secure as the 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 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 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 these vulnerabilities. These vulnerabilities have high attack complexity.

6 CONTACT INFORMATION

Recipients of this report are encouraged to contribute any additional information that 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

7 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