ICSMA-24-XXX-XX

Baxter Welch Allyn Configuration Tool

View CSAF

1. EXECUTIVE SUMMARY

CVSS v3 9.6

- **ATTENTION**: Exploitable remotely
- **Vendor**: Baxter
- **Equipment**: Welch Allyn Configuration Tool
- **Vulnerability**: Insufficiently Protected Credentials

2. RISK EVALUATION

Successful exploitation of this vulnerability could lead to the unintended exposure of credentials to unauthorized users.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following Baxter (formerly Hillrom and Welch Allyn) products, are affected:

- Welch Allyn Product Configuration Tool: Versions 1.9.4.1 and prior

3.2 Vulnerability Overview

3.2.1 INSUFFICIENTLY PROTECTED CREDENTIALS CWE-522

Any credentials that were used for authentication or input while using the Welch Allyn

Configuration Tool have the potential to be compromised and should be changed immediately.

CVE-2024-5176 has been assigned to this vulnerability. A CVSS v3.1 base score of 9.6 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:L).

A CVSS v4 score has also been calculated for CVE-2024-5176. A base score of 9.4 has been calculated; the CVSS vector string is (CVSS4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:L/SC:H/SI:H/SA:L).

3.3 BACKGROUND

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

3.4 RESEARCHER

Baxter reported this vulnerability to CISA.

4. MITIGATIONS

Baxter will release a software update for all impacted software to address this vulnerability. A new version of the product that mitigates the vulnerability will be available as follows:

- Welch Allyn Product Configuration Tool versions 1.9.4.2: Available Q3 2024
- No user action will be required once the update is released.

Baxter recommends the following workarounds to help reduce risk:

- Apply proper network and physical security controls.
- The Welch Allyn Configuration Tool has been removed from public access. Customers are advised to contact Baxter Technical Support or their Baxter Project Manager to create configuration files, as needed. Baxter Technical Support can be reached at (800)535-6663, option 2.

CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability, such as:

- Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the internet.
- Locate control system networks and remote devices behind firewalls and isolating them from business networks.
- When remote access is required, use more 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 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/ics. Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets.

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

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

No known public exploitation specifically targeting this vulnerability has been reported to CISA at this time.

5. UPDATE HISTORY

- May 30, 2024: Initial Publication