Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

HC3: Sector Alert

June 04, 2024 TLP:CLEAR Report: 202406041700

Baxter Welch Allyn Vulnerabilities

Executive Summary

CISA recently published two ICS Medical Advisories for Baxter products, including Baxter Welch Allyn Configuration Tool and Baxter Welch Allyn Connex Spot Monitor (CSM). Both vulnerabilities received a CVSS v4 score of 9 or higher (CRITICAL), and are exploitable remotely. Successful exploitation of one of these vulnerabilities could result in an impact and/or delay to patient care. While a patch is currently available for one of these vulnerabilities, a software update will not be made available for the other until Q3 2024. Mitigations and workarounds from the vendor and CISA are outlined in this Sector Alert.

Report

On May 30, 2024, CISA published multiple ICS Medical Advisories for Baxter products and medical devices. The affected products include Baxter Welch Allyn Configuration Tool (versions 1.9.4.1 and prior) and Baxter Welch Allyn Connex Spot Monitor (CSM) (versions 1.52 and prior). Both vulnerabilities (detailed in the Vulnerabilities section) received a CVSS v4 score of 9 or higher and are exploitable remotely. Successful exploitation of these vulnerabilities could lead to the unintended exposure of credentials to unauthorized users and/or allow an attacker to modify device configuration and firmware data. Tampering with this data could lead to device compromise, resulting in impact and/or delay in patient care. According to Baxter: “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.” Despite this risk, Baxter stated that it has not found any evidence to suggest the flaw has been exploited in the wild, and plans to release a new software update to address the flaw in Q3 2024.

Analysis

These two vulnerabilties involve multiple common weaknesses. The first is “CWE-522: Insufficiently Protected Credentials” in which the product transmits or stores authentication credentials, but it uses an insecure method that is susceptible to unauthorized interception and/or retrieval. Automated static analysis, commonly referred to as Static Application Security Testing (SAST), can find some instances of this weakness by analyzing source code (or binary/compiled code) without having to execute it. Typically, this is done by building a model of data flow and control flow, then searching for potentially-vulnerable patterns that connect “sources” (origins of input) with “sinks” (destinations where the data interacts with external components, a lower layer such as the OS, etc.). The second is “CWE-1394: Use of Default Cryptographic Key” in which product uses a default cryptographic key for potentially critical functionality. It is common practice for products to be designed to use default keys. The rationale is to simplify the manufacturing process or the system administrator’s task of installation and deployment into an enterprise. However, if admins do not change the defaults, it is easier for attackers to bypass authentication quickly across multiple organizations.

Vulnerabilities

- CVE-2024-5176 (CVSS v4 9.4): Insufficiently Protected Credentials (CWE-522) vulnerability in Baxter Welch Allyn Configuration Tool may allow Remote Services with Stolen Credentials. This issue affects Welch Allyn Configuration Tool: versions 1.9.4.1 and prior.
- CVE-2024-1275 (CVSS v4 9.1): Use of Default Cryptographic Key (CWE-1394) vulnerability in Baxter Welch Ally Connex Spot Monitor may allow Configuration/Environment Manipulation. This issue affects Welch Ally Connex Spot Monitor in all versions prior to 1.52.

Patches, Mitigations, and Workarounds

Baxter Welch Allyn Configuration Tool (versions 1.9.4.1 and prior): Baxter has found no evidence to date of any compromise of personal or health data. 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 isolate 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.

Baxter Welch Allyn Connex Spot Monitor (CSM) (versions 1.52 and prior): Baxter has released a software update for all impacted devices and software to address this vulnerability. A new version of the product that mitigates the vulnerability is available as follows:

- Welch Allyn Connex Spot Monitor: Version 1.52.01 (available October 16, 2023)

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

Baxter recommends the following workarounds to help reduce risk:

- Apply proper network and physical security controls.
- Ensure a unique encryption key is configured and applied to the product (as described in the Connex Spot Monitor Service Manual).

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.

References

Alder, Steve. "Critical Vulnerabilities Identified in Baxter Welch Allyn Products." HIPAA Journal. May 31, 2024. https://www.hipaajournal.com/critical-vulnerabilities-baxter-welch-allyn-05-24/

CISA. "ICS Medical Advisory: Baxter Welch Allyn Configuration Tool (ICSMA-24-151-01)." May 30, 2024. https://www.cisa.gov/news-events/ics-medical-advisories/icsma-24-151-01

CISA. "ICS Medical Advisory: Baxter Welch Allyn Connex Spot Monitor (ICSMA-24-151-02)." May 30, 2024. https://www.cisa.gov/news-events/ics-medical-advisories/icsma-24-151-02

NIST. "National Vulnerability Database, Vulnerability Detail, CVE-2024-5176." May 29, 2024. https://nvd.nist.gov/vuln/detail/CVE-2024-5176

NIST. "National Vulnerability Database, Vulnerability Detail, CVE-2024-1275." May 29, 2024. https://nvd.nist.gov/vuln/detail/CVE-2024-1275

Mitre. "Common Weakness Enumeration, CWE-522: Insufficiently Protected Credentials." https://cwe.mitre.org/data/definitions/522.html

Mitre. "Common Weakness Enumeration, CWE-1394: Use of Default Cryptographic Key." https://cwe.mitre.org/data/definitions/1394.html

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback