ICSMA-24-XXX-XX

Baxter Welch Allyn Connex Spot Monitor

View CSAF

1. EXECUTIVE SUMMARY

CVSS v4 9.1

- **ATTENTION**: Exploitable remotely
- **Vendor**: Baxter
- **Equipment**: Welch Allyn Connex Spot Monitor (CSM)
- **Vulnerability**: Use of Default Cryptographic Key

2. RISK EVALUATION

Successful exploitation of this vulnerability could 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.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following Baxter (formerly manufactured by Hillrom) medical devices are affected:

- Welch Allyn Connex Spot Monitor (CSM): Versions 1.52 and prior

3.2 Vulnerability Overview

3.2.1 USE OF DEFAULT CRYPTOGRAPHIC KEY CWE-1394

The impacted product uses a default cryptographic key for potentially critical functionality. An attacker could modify device configurations and firmware data, resulting in impact and/or delay in patient care

CVE-2024-1275 has been assigned to this vulnerability. A CVSS v3.1 base score of 7.4 has been calculated; the CVSS vector string is (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).

A CVSS v4 score has also been calculated for CVE-2024-1275. A base score of 9.1 has been calculated; the CVSS vector string is (CVSS4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N).

3.3 BACKGROUND

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

3.4 RESEARCHER

Maarten Boone and Edwin Van Andel (CTO of Zerocopter) reported this vulnerability to Baxter.

4. MITIGATIONS

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 1.5.2.01 (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.

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