Baxter Connex Health Portal

Release Date: Sept 05, 2024
Alert Code: ICSMA-24-249-XX

1. EXECUTIVE SUMMARY

CVSS v3.1 10

ATTENTION: Exploitable remotely/low attack complexity

Vendor: Baxter

Equipment: Connex Health Portal

Vulnerability: SQL Injection, Improper Access Control

2. RISK EVALUATION

Successful exploitation of these vulnerabilities could lead to malicious code injection, shutdown of database service, or the ability to access, modify, or delete sensitive data from the database.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

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

Baxter Connex Health Portal: all versions prior to 8/30/2024

3.2 Vulnerability Overview

3.2.1 IMPROPER NEUTRALIZATION OF SPECIAL ELEMENTS USED IN AN SQL COMMAND ('SQL INJECTION') CWE-89

Due to improper sanitation of values of certain parameters, a remote, unauthenticated attacker could potentially run arbitrary SQL queries, access, modify and delete sensitive data and/or administrative operations including shutting down the database.

CVE-2024-6795 has been assigned to this vulnerability. A CVSS v3.1 base score of 10 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

3.2.2 IMPROPER ACCESS CONTROL CWE-284

A vulnerability in the application could potentially lead to an unauthorized user gaining access to patient and clinician information, modifying or deleting clinic details.

CVE-2024-6796 has been assigned to this vulnerability. A CVSS v3.1 base score of 8.2 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N).

3.3 BACKGROUND

CRITICAL INFRASTRUCTURE SECTORS: Healthcare and Public Health

COUNTRIES/AREAS DEPLOYED: United States

COMPANY HEADQUARTERS LOCATION: United States

3.4 RESEARCHER

Baxter reported this vulnerability to CISA.

4. MITIGATIONS

Baxter is unaware of any exploitation of these vulnerabilities and/or the compromise of personal or health data. No user action is required.

Baxter recommends the following workarounds to help reduce risk:

These vulnerabilities were patched promptly after discovery and no additional user action is required.

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

CISA also recommends users take the following measures to protect themselves from social engineering attacks:

Do not click web links or open attachments in unsolicited email messages.
Refer to Recognizing and Avoiding Email Scams for more information on avoiding email scams.

Refer to Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks.

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

5. UPDATE HISTORY

Sept 05, 2024: Initial Publication