ICSMA-24-319-01

Baxter Life2000 Ventilation System

View CSAF

1. EXECUTIVE SUMMARY

CVSS v4 10.0

- **ATTENTION:** Exploitable remotely/low attack complexity
- **Vendor:** Baxter
- **Equipment:** Life2000 Ventilation System

Vulnerabilities: Cleartext Transmission of Sensitive Information, Improper Restriction of Excessive Authentication Attempts, Use of Hard-Coded Credentials, Improper Physical Access Control, Download of Code Without Integrity Check, On-Chip Debug and Test Interface With Improper Access Control, Missing Support for Security Features in On-Chip Fabrics or Buses, Missing Authentication for Critical Function, Insufficient Logging

2. RISK EVALUATION

Successful exploitation of these vulnerabilities could lead to information disclosure and/or disruption of the device's function without detection.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following Baxter (formerly Hillrom) products are affected:

- Life2000 Ventilation System: All versions prior to and including 06.08.00.00

3.2 Vulnerability Overview

3.2.1 CLEARTEXT TRANSMISSION OF SENSITIVE INFORMATION (CWE-319)

Improper data protection on the ventilator's serial interface could allow an attacker to send and receive messages that result in unauthorized disclosure of information and/or have unintended impacts on device settings and performance.

CVE-2024-9834 has been assigned to this vulnerability. A CVSS v3.1 base score of 9.3 has been calculated; the CVSS vector string is (AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

A CVSS v4 score has also been calculated for CVE-2024-9834. A base score of 9.4 has been calculated; the CVSS vector string is (CVSS4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H).

3.2.2 IMPROPER RESTRICTION OF EXCESSIVE AUTHENTICATION ATTEMPTS (CWE-307)

There is no limit on the number of failed login attempts permitted with the Clinician Password or the Serial Number Clinician Password. An attacker could execute a brute-force attack to gain unauthorized access to the ventilator, and then make changes to device settings that could disrupt the function of the device and/or result in unauthorized information disclosure.

CVE-2024-9832 has been assigned to this vulnerability. A CVSS v3.1 base score of 9.3 has been calculated; the CVSS vector string is (AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

A CVSS v4 score has also been calculated for CVE-2024-9832. A base score of 9.4 has been calculated; the CVSS vector string is (CVSS4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H).

3.2.3 USE OF HARD-CODED CREDENTIALS (CWE-798)

The Clinician Password and Serial Number Clinician Password are hard-coded into the ventilator in plaintext form. This could allow an attacker to obtain the password off the ventilator and use it to gain unauthorized access to the device, with clinician privileges.

CVE-2024-48971 has been assigned to this vulnerability. A CVSS v3.1 base score of 9.3 has been calculated; the CVSS vector string is (AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

A CVSS v4 score has also been calculated for CVE-2024-48971. A base score of 9.4 has been calculated; the CVSS vector string is (CVSS4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H).

3.2.4 IMPROPER PHYSICAL ACCESS CONTROL (CWE-1263)

The debug port on the ventilator's serial interface is enabled by default. This could allow an attacker to send and receive messages over the debug port (which are unencrypted; see 3.2.1) that result in unauthorized disclosure of information and/or have unintended impacts on device settings and performance.

CVE-2024-48973 has been assigned to this vulnerability. A CVSS v3.1 base score of 9.3 has been calculated; the CVSS vector string is (AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

A CVSS v4 score has also been calculated for CVE-2024-48973. A base score of 9.4 has been calculated; the CVSS vector string is (CVSS4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H).

3.2.5 DOWNLOAD OF CODE WITHOUT INTEGRITY CHECK (CWE-494)

The ventilator does not perform proper file integrity checks when adopting firmware updates. This makes it possible for an attacker to force unauthorized changes to the device's configuration settings and/or compromise device functionality by pushing a compromised/illegitimate firmware file. This could disrupt the function of the device and/or cause unauthorized information disclosure.

CVE-2024-48974 has been assigned to this vulnerability. A CVSS v3.1 base score of 9.3 has been calculated; the CVSS vector string is (AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

A CVSS v4 score has also been calculated for CVE-2024-48974. A base score of 9.4 has been calculated; the CVSS vector string is (CVSS4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H).

3.2.6 ON-CHIP DEBUG AND TEST INTERFACE WITH IMPROPER ACCESS CONTROL (CWE-1191)

The ventilator's microcontroller lacks memory protection. An attacker could connect to the internal JTAG interface and read or write to flash memory using an off-the-shelf debugging tool, which could disrupt the function of the device and/or cause unauthorized information disclosure.

CVE-2024-48970 has been assigned to this vulnerability. A CVSS v3.1 base score of 9.3 has been calculated; the CVSS vector string is (AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

A CVSS v4 score has also been calculated for CVE-2024-48970. A base score of 9.4 has been calculated; the CVSS vector string is (CVSS4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H).

3.2.7 MISSING SUPPORT FOR SECURITY FEATURES IN ON-CHIP FABRICS OR BUSES (CWE-1318)

The flash memory read-out protection feature on the microcontroller does not block memory access via the ICode bus. Attackers can exploit this in conjunction with certain CPU exception handling behaviors to gain knowledge of how the onboard flash memory is organized and ultimately bypass read-out protection to expose memory contents.

CVE-2020-8004 has been assigned to this vulnerability. A CVSS v3.1 base score of 7.5 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).

A CVSS v4 score has also been calculated for CVE-2020-8004. A base score of 6.9 has been calculated; the CVSS vector string is (CVSS4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N).

3.2.8 MISSING AUTHENTICATION FOR CRITICAL FUNCTION (CWE-306)

The software tools used by service personnel to test & calibrate the ventilator do not support user authentication. An attacker with access to the Service PC where the tools are installed could obtain diagnostic information through the test tool or manipulate the ventilator's settings and embedded software via the calibration tool, without having to authenticate to either tool. This could result in unauthorized disclosure of information and/or have unintended impacts on device settings and performance.

CVE-2024-48966 has been assigned to this vulnerability. A CVSS v3.1 base score of 10.0 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

A CVSS v4 score has also been calculated for CVE-2024-48966. A base score of 10.0 has been calculated; the CVSS vector string is (CVSS4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H).

3.2.9 INSUFFICIENT LOGGING (CWE-778)

The ventilator and the Service PC lack sufficient audit logging capabilities to allow for detection of malicious activity and subsequent forensic examination. An attacker with access to the ventilator and/or the Service PC could, without detection, make unauthorized changes to ventilator settings that result in unauthorized disclosure of information and/or have unintended impacts on device performance.

CVE-2024-48967 has been assigned to this vulnerability. A CVSS v3.1 base score of 10.0 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

A CVSS v4 score has also been calculated for CVE-2024-48967. A base score of 10.0 has been calculated; the CVSS vector string is (CVSS4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H).

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 these vulnerabilities to CISA.

4. MITIGATIONS

Baxter plans to issue a follow-up announcement in Q2 2025 regarding the Life2000 vulnerabilities described in this disclosure.

Baxter is unaware of any exploitation of these vulnerabilities and/or the compromise of personal or health data.

Baxter recommends that users of the Life2000 Ventilation System not leave their ventilators unattended in public or unsecured areas. Maintaining physical possession and control of the ventilator reduces the likelihood of a malicious actor gaining access to the device.

For more information, refer to Baxter's Product Security and Responsible Disclosures web page.

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 these vulnerabilities has been reported to CISA at this time.

5. UPDATE HISTORY

- November 14, 2024: Initial Publication