Bonaduz, May 28, 2021

# Product Security Advisory – PSA-2021-02

## 1. Introduction

During our regular vulnerability monitoring procedure we discovered an issue with multiple operating systems (https://us-cert.cisa.gov/ics/advisories/icsa-21-119-04).

Hamilton Medical is aware, that the "BadAlloc" vulnerability was found in VxWorks and ARM CMSIS operating systems (RTOS) which is used by some of our products.

Hamilton Medical has conducted an impact analysis and risk assessment, and has identified no patient risks associated with these vulnerabilities.

## 2. Affected Products

The following Hamilton Medical products are affected by the identified vulnerabilities:

- HAMILTON-C1/T1/MR1
- HAMILTON-C2
- HAMILTON-C3
- HAMILTON-C6
- HAMILTON-G5/S1

## 3. Vulnerability Description

The following section refers to the US-CERT advisory ICSA-21-119-04, which is published online at: https://www.us-cert.gov/ics/advisories

### 1. Integer overflow or wraparound CWE-190

ARM CMSIS RTOS2 versions prior to 2.1.3 are vulnerable to integer wrap-around inosRtxMemoryAlloc (local malloc equivalent) function, which can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or injected code execution.

CVE-2021-27431 has been assigned to this vulnerability. A CVSS v3 base score of 7.3 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).

### 2. Integer overflow or wraparound CWE-190

Wind River VxWorks several versions prior to 7.0 firmware is vulnerable to weaknesses found in the following functions; calloc(memLib), mmap/mmap64 (mmanLib), cacheDmaMalloc(cacheLib) and cacheArchDmaMalloc(cacheArchLib). This improper memory assignment can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or a remote code injection/execution.

CVE-2020-35198 and CVE-2020-28895 have been assigned to this vulnerability. A CVSS v3 base score of 7.3 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).

Hamilton Medical AG
Via Crusch 8, 7402 Bonaduz
Switzerland

☎ +41 58 610 10 20
info@hamilton-medical.com
**www.hamilton-medical.com**

## 4. Impact

An impact analysis and risk assessment has identified no patient risks associated with the vulnerabilities. All vulnerabilities require physical access to the device.

- **Integer overflow or wraparound**

Devices have limited memory available and the application will never alloc a memory amount which leads to a memory corruption. There is no interface that allows users to remotely control memory allocation.

All Hamilton Medical ventilators except HAMILTON-C1/T1 > V3.0.0 are not connected via Ethernet to a network and/or the internet. There is an RS232 connection possibility for outgoing data only (no bi-directional communication).

HAMILTON-C1/T1 > 3.0.0 may be connected via Ethernet or WiFi to a network and/or the internet. The connection is protected by an independent module between the ventilator and the network. This module does not use an affected operating system.

## 5. Mitigation

No customer interventions are necessary. In general, Hamilton Medical recommends:

- Prevent physical access to the device by unauthorized personnel
- Pay attention to notifications, alarms, and alerts
- Use only software from official Hamilton Medical channels and have it installed by an authorized technician

As part of the continuous product care and maintenance process, Hamilton Medical will provide fixes for vulnerabilities. Due to the risk profile, as well as technical feasibility, Hamilton Medical will not provide an immediate fix for these vulnerabilities. The patches provided by the RTOS vendors will be included in the regular software updates.

Hamilton Medical AG
Via Crusch 8, 7402 Bonaduz
Switzerland

☎ +41 58 610 10 20
info@hamilton-medical.com
**www.hamilton-medical.com**

## 6. Contact Information

For further questions regarding the impact or mitigation of the vulnerabilities, please contact your local sales or service manager. Alternatively, you can directly contact Hamilton Medical at:

product-security.med.global@hamilton-medical.com

**Revisions**

| Revision | Publication date | Updates |
|---|---|---|
| 1.0 | 2021-05-26 | Initial version |

**Released by**

| | |
|---|---|
| **Hollenberg Sebastian**<br>Product Management | **Annemarie Weideli**<br>Team Leader Regulatory Affairs |
| Hollenberg Sebastian Alexander 2195<br>Digitally signed by Hollenberg Sebastian Alexander 2195<br>Date: 2021.05.31 08:37:24 +02'00' | Weideli Annemarie 1622<br>Digital unterschrieben von Weideli Annemarie 1622<br>Datum: 2021.05.31 09:49:33 +02'00' |

Hamilton Medical AG
Via Crusch 8, 7402 Bonaduz
Switzerland

☎ +41 58 610 10 20
info@hamilton-medical.com
**www.hamilton-medical.com**