Bonaduz, February 25, 2021

Product Security Advisory – PSA-2021-01

1. Introduction

Hamilton Medical participated in the project ManiMed (Manipulation of Medical Devices) that was initiated by the Federal Office for Information Security (BSI, Germany) to raise awareness for IT security risks of networked medical devices. As part of the ManiMed project, the HAMILTON-T1 was evaluated for product security vulnerabilities. In total, three vulnerabilities have been identified which allow attackers with physical access to the device to obtain sensitive information or to put the device into an undefined state. See section 3 for a detailed description of the vulnerabilities.

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 (software version 2.2.X or earlier)
- HAMILTON-C2
- HAMILTON-C3
- HAMILTON-C6
- HAMILTON-G5/S1

3. Vulnerability Description

The following section refers to the US-CERT advisory ICSMA-21-047-01, which is published online at: https://www.us-cert.gov/ics/advisories

1. Use of Hard-Coded Credentials CWE-798

The use of hard-coded credentials allows attackers with physical access to the device to obtain access to the configuration interface of the ventilator. A CVSSS v.3 base score of 3.5 was calculated.

2. Missing XML Validation CWE-112

An XML validation vulnerability in the ventilator allows privileged attackers with physical access to render the device persistently unusable by uploading modified configuration files. A CVSS v.3 base score of 4.3 was calculated.

3. Exposure of sensitive information to an unauthorized actor CWE-200

An information disclosure vulnerability in the ventilator allows attackers with physical access to the configuration interface' logs to get valid checksums for tampered configuration files. A CVSS v.3 base score of 2.4 was calculated.

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.

- **Use of Hard-Coded Credentials**

The use of hard-coded credentials allow attackers with physical access to obtain access to the configuration interface of the ventilator. The configuration interface is used to configure standard settings and load configuration files and presets. The configuration interface does not provide means to manipulate ventilation settings that will result in patient harm.

- **Missing XML Validation**

A modified configuration file can lead to a DoS attack in which the ventilator is not able to restart, and needs to be serviced by an authorized technicians. Loading configuration files is only possible when in Standby mode, when no patient is connected to the ventilator. Therefore, the vulnerability does not result in patient harm.

- **Exposure of sensitive information to an unauthorized actor**

The ventilator supports the export of configuration files. Configuration files are not intended to be edited or modified. To protect against modification, the configuration file is protected by a checksum. Should a modified configuration file be imported, the ventilator will reject it and write the calculated and expected checksum to a file. It protects against accidental data corruption and is not considered a security feature. Configuration files can only be loaded during standby. The configuration files only provides default control settings, however alarm settings cannot be preconfigured by a configuration file. Harmful settings would immediately result in an alarm notification.

5. Mitigation

As the impact of the identified vulnerabilities is negligible, 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 the following vulnerabilities: *"Missing XML Validation CWE-112"* and *"Exposure of sensitive information to an unauthorized actor CWE-200"*. Due to the risk profile, as well as technical feasibility, Hamilton Medical will not provide a fix for the vulnerability: *"Use of Hard-Coded Credentials CWE-798"*. The fixes will be available for the following products with the corresponding software version or higher.

- HAMILTON-C1/T1/MR1: software version 3.0.0 or higher
- HAMILTON-C3: software version 2.1.0 (expected in Q3/2021)
- HAMILTON-C6: software version 1.2.0 (expected in Q3/2021)
- HAMILTON-G5/S1: software version 2.90 (expected in Q4/2021)

The availability of the software versions is subject to local registration. Hamilton Medical recommends always using the products with latest available software version.

Hamilton Medical AG
Via Crusch 8, 7402 Bonaduz
Switzerland

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

6. Credit

The identified vulnerabilities were reported by Julian Suleder, Birk Kauer, Raphael Pavlidis, and Nils Emmerich of ERNW Research GmbH to the Federal Office for Information Security (BSI, Germany) in the context of the BSI project ManiMed, in which Hamilton Medical AG participated.

7. 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	2021-02-23	Initial version
1.1	2021-02-25	Reference to HAMILTON-C1/T1/MR1 software version 2.2.X is added

Released by

Dr. Lorenz Stähle Group Teamleader Digital Solutions	**Annemarie Weideli** Team Leader Regulatory Affairs
	

Hamilton Medical AG
Via Crusch 8, 7402 Bonaduz
Switzerland

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