Bonaduz, February 22, 2024

Company Statement

Security of Hamilton Medical devices

To whom it may concern

This statement explains the security considerations of Hamilton Medical devices concerning product lines with following product numbers (PN).

Product line	Product number	Serial number
HAMILTON-C1	PN 161001 PN 1610010*	All
HAMILTON-C2	PN 160001	
HAMILTON-C3	PN 160005	
HAMILTON-C6	PN 160021	
HAMILTON-G5	PN 159001 PN 159002 PN 159003	
HAMILTON-MR1	PN 161010 PN 1610100	
HAMILTON-S1	PN 159005 PN 159005NK PN 159005MA PN 159007	
HAMILTON-T1	PN 161006 PN 161009 PN 1610060* PN 1610090*	
	* = with Hamilton Connect Module	

Hamilton Medical AG
Via Crusch 8, 7402 Bonaduz
Switzerland

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

1. Hardware

This chapter describes the hardware safeguard.

1.1. Secure elements (SE) for hardware

Whenever possible, cryptographic keys are stored in hardware by a secure element.

NOTE: This depends on the hardware generation of a device. In general, newer devices employ this technique more widely than older devices. This is applicable especially to devices, which are equipped with the Hamilton Connect Module.

2. Software

This chapter describes the software safeguards.

2.1. Secure elements (SE) for software and security updates

With regular operating system and software bug fixes for Hamilton Medical devices, Hamilton Medical conforms to current software standards to ensure that all devices are protected and secure.

NOTE: Hamilton Medical reserves the right to not update discontinued product lines.

2.2. Virus scanner and intrusion detection system (IDS)

Hamilton Medical devices do neither employ virus scanning nor intrusion detection system technology due to a likely impact on device performance and thus patient safety. However, the resilience against viruses, malware and ransomware are deemed sufficient to make such technologies unnecessary.

2.3. Resilience against viruses/malware/ransomware

The following instruments are applied to build resilience against viruses, malware and ransomware.

1. **Hardened operating system**
   Most common viruses, malware and ransomware are only effective on widely used operating systems such as Windows, Mac OS, or Linux. Hamilton Medical devices do not use any of these operating systems. Hamilton Medical devices use an embedded operating system, which has been developed specifically for industries requiring a high level of safety and security such as aerospace, defense, industrial equipment, and medical devices. Hardening of the operating system is applied additionally.

2. **Signed software** (HAMILTON-C1/T1/MR1 with SW version 3.0.x or higher; HAMILTON-C6)
   All software packages to be installed on a Hamilton Medical device are cryptographically signed. Signatures are validated prior to installation to prevent installation from unknown sources.

3. **“Install from unknown sources” is strictly prohibited**
   An option to “Install from unknown sources” (like Android or other mobile systems) is not available and cannot be activated.

4. **Whitelisting**
   Hamilton Medical uses whitelisting. Only predefined files will be loaded by the system.

5. **Checksum**
   All executable files are verified with a checksum for validity during startup.

Hamilton Medical AG
Via Crusch 8, 7402 Bonaduz
Switzerland

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

3. Communication interfaces

This chapter describes the safeguards related to communication interfaces in detail.

3.1. **RS-232 for device-2-device communication** (NOT HAMILTON-MR1)

There is an RS-232 connection possibility for outgoing data only. No bi-directional communication or remote control are available by design.

3.2. Universal Serial Bus (USB)

With removable media such as an USB stick, malware will not be executed on a Hamilton Medical device, because:

1. **Mass storage device only** (Memory sticks)
   Only mass storage USB devices are supported.

2. **No auto-start**
   Files are neither automatically read nor executed without explicit user interaction (e.g., software update performed by service technician).

3. **Write-Only while ventilating**
   Hamilton Medical devices use USB mass storage devices in write-only mode during ventilation. During ventilation no data is read from the USB. The device only reads from USB in service mode or standby mode.

3.3. **Ethernet** (Devices with/without Hamilton Connect Module; NOT HAMILTON-MR1)

Built-in Ethernet is only used in manufacturing, disabled prior to shipment, and cannot be re-enabled afterwards.

3.4. **Ethernet, WLAN, Bluetooth, NFC** (Devices with Hamilton Connect Module)

Hamilton Medical devices equipped with Hamilton Connect Module (HCM) apply additional safeguards to networked interfaces:

1. **Development: UL 2900 testing**
   Software is developed and tested according to
   a. UL 2900-1, “Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements”
   b. UL 2900-2-1, “Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems”

2. **Hardware: Dedicated hardware resources**
   Communication is performed on dedicated and independent hardware to the ventilator.

3. **Network interfaces: Encryption and Authentication of connection** (Data-in-transit)
   Each interface uses industry standard cryptography to authenticate as well as encrypt data-in-transit.

4. **Network: Firewall**
   A firewall blocks all communication except if user actions require communication. Only necessary communication is allowed, all other communication is blocked.

Hamilton Medical AG
Via Crusch 8, 7402 Bonaduz
Switzerland

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

5. **Protocol: Encryption and Authentication** (Data-in-transit)
   On top of network interface security, additional encryption and authentication is performed on protocol level whenever possible. Algorithms compliant with current BSI TR-02102 and NIST SP 800-57 part 1 are employed.
   NOTE: Not all supported protocols or 3rd party products support encryption or authentication of data-in-transit

6. **Protocol: No remote control**
   By design, the HCM cannot remote control or influence the ventilation process in any way.

7. **Data: Encryption** (Data-at-rest)
   Encryption is applied to data exported to USB mass storage devices by HCM.

8. **Passive NFC**
   NFC is only active if user actions require it. In addition, NFC is used in passive mode only. This means data transition must be initiated by an NFC reader and no active transmission is performed otherwise.

4. Continuous monitoring

This chapter provide a list of processes for continuous monitoring.

4.1. Monitoring and security scanning

Hamilton Medical constantly monitors evolving threats and employs various security scanning methods and technologies. In addition, Hamilton Medical started to test devices[1] by independent parties.

4.2. Security advisories

Hamilton Medical releases security advisories to the public in case a potential vulnerability was identified.

NOTE: For further information see https://www.hamilton-medical.com/Services/Cybersecurity.html

4.3. Product Security Incidence Response Team (PSIRT)

Hamilton Medical employs trained security personnel to react to product security incidents.

NOTE: To report a security issue, please get in touch with Hamilton Medical PSIRT by filing a report through https://www.hamilton-medical.com/Services/Cybersecurity.html

NOTE: Hamilton Medical follows a responsible disclosure procedure. Hamilton Medical highly encourages security researchers to get in contact and does not retaliate in any way against whistleblowers or reports being submitted.

With kind regards

Hamilton Medical AG

Schumann Janek 23846
Digitally signed by Schumann Janek 23846
Date: 2024.02.22 19:48:06 +01'00'

Janek Schumann

Product Security Officer
product-security.med.global@hamilton-medical.com

Hoeft Annemarie 1622
Digital unterschrieben von Hoeft Annemarie 1622
Datum: 2024.02.27 15:58:47 +01'00'

Annemarie Höft

Head of Regulatory Affairs
regulatory.med.global@hamilton-medical.com

[1] 2023: HAMILTON-C6