SPACELABS
HEALTHCARE

23 May 2017

WannaCry Malware Vulnerability Assessment and Microsoft Patch Compatibility Statement

In response to the rapid global proliferation of malicious software known as WannaCry (also known as WCry, or Wanna Decryptor), Spacelabs has conducted an assessment to identify potential vulnerabilities in our products to this attack. We evaluated if the product is vulnerable to the ransomware encryption attack, or if the attack could spread through the product.

Details about the WannaCry ransomware attack are described in US-CERT Alert TA17-123A: Indicators Associated with WannaCry Ransomware, and details about the vulnerabilities to Microsoft Windows systems have been published by Microsoft via Technet: https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/.

To date, we have no reports from customers that their Spacelabs product(s) have been affected by the WannaCry malware. Nevertheless, we recommend that your IT staff review the following assessment of our current product portfolio and software versions and take actions as appropriate for your network environment. Note that the host platform of some systems could be affected if the hospital network becomes compromised. As part of good IT hygiene, we recommend that customers maintain current patching on the hospital network.

Our older products and software versions are based on comparable architecture to current products and software versions. Where we have determined that the current product/software version is not vulnerable, we believe that our older products will also not be directly susceptible to WannaCry attacks. Nevertheless, we are continuing to review historical product releases and will issue assessments as appropriate.

Please contact Spacelabs Technical Support if you require more information than is provided in the table below, or contact us through our country offices or representatives.

Spacelabs Technical Support
United States: +1 (800) 522-7025 | techsupport@spacelabs.com
EMEA: emea.techsupport@spacelabs.com

Patient Monitoring and Connectivity Products

Product	Findings and Recommendations
Bedside Monitors: • Xprezzon 91393 • Qube 91390 • Ultraview SL	Not vulnerable due to system architecture.
• XTR 96280	XTR is vulnerable to the WannaCry attack if it is connected to a network that has been compromised. In this instance, the XTR device could become encrypted or allow the attack to spread through it. You can reduce the risk to your network and these device by installing the recommended Microsoft patch to computers running Windows on the hospital network. Spacelabs has expedited the release of a product update that will remove this vulnerability.
• Xhibit 96102	Not vulnerable due to system architecture.

Product	Findings and Recommendations
• Xprezznet 96190	Spacelabs XprezzNet 1.3.2 software is not directly vulnerable to this attack, however the customer managed host platform could be affected. Customers should proceed to patch their Windows platforms as recommended by Microsoft. Xprezznet 1.3.2 has been tested on all OS configurations defined in the minimum installation instructions (Windows Server 2008 R2 or 2012 R2) with Microsoft MS17-010 patch applied. Testing confirmed that the patch does not impact the operation of the software.
• Intesys Clinical Suite (ICS)	Spacelabs ICS 5.2.2 software is not directly vulnerable to this attack, however the customer managed host platform could be affected. Customers should proceed to patch their Windows platforms as recommended by Microsoft. ICS 5.2.2 has been tested on all OS configurations defined in the minimum installation instructions (Windows Server 2012 R2, and Clinical Access clients installed on Windows 7 or 8.1) with Microsoft MS17-010 patch applied. Testing confirmed that the patch does not impact the operation of the software.

Diagnostic Cardiology Products

Product	Findings and Recommendations
• Cardiology ECG & ABM Units	Not vulnerable due to system architecture.
• Pathfinder	Spacelabs Pathfinder software is not directly vulnerable to this attack, however the customer managed host platform could be affected. Customers should proceed to patch their Windows platforms as recommended by Microsoft. Pathfinder 1.8 has been tested on all supported OS configurations (Windows 7, 8.1. and 10) with Microsoft MS17-010 patch applied. Testing confirmed that the patch does not impact the operation of the software.
• Sentinel	Spacelabs Sentinel software is not directly vulnerable to this attack, however the customer managed host platform could be affected. Customers should proceed to patch their Windows platforms as recommended by Microsoft. Sentinel 10 has been tested on all supported OS configurations (Windows 7, 8.1. and 10) with Microsoft MS17-010 patch applied. Testing confirmed that the patch does not impact the operation of the software.

Anesthesia Delivery and Ventilation Products

Product	Findings and Recommendations
• ARKON	Not vulnerable due to system architecture.
• Blease900	Not vulnerable due to system architecture.
• Blease700	Not vulnerable due to system architecture.