SPACELABS HEALTHCARE

Security Advisory

Urgent-11 Vulnerability VxWorks Impacts Spacelabs Monitors

Ref Doc ID	Version	Release Date	Advisory Status	Related CVE(s)	Sev Rating CVSS 3	Operational Risk
CSN 079-0233-00	Rev A	10 October 2019	ACTIVE	CVE-2019-12256 CVE-2019-12257 CVE-2019-12255 CVE-2019-12260 CVE-2019-12261 CVE-2019-12263 CVE-2019-12258 CVE-2019-12259 CVE-2019-12262 CVE-2019-12264 CVE-2019-12265	9.8 8.8 9.8 9.8 8.8 8.1 7.5 6.3 7.1 7.1 5.4	

1. INTRODUCTION

VxWorks is a Real Time Operating System developed and supported by WindRiver Corporation. VxWorks is widely used and can be found in thousands of models of equipment in the aerospace, defense, automotive, medical, networking and communications industries. VxWorks is also used in certain Spacelabs Healthcare products.

In a coordinated vulnerability disclosure process, on July 29, 2019, Armis, an enterprise security firm, and WindRiver publicized information regarding a set of 11 vulnerabilities in the IPNet service that is in the VxWorks Operating System. These eleven vulnerabilities are known collectively by the name “Urgent-11”.

2. AFFECTED PRODUCTS

Spacelabs has determined that the following products could be impacted by these vulnerabilities.

- Current Spacelabs bedside monitors (Xprezzon, Qube, Qube Mini), which use VxWorks 6.6.
- Older UVSL Spacelabs bedside and central monitors which used VxWorks 6.6 as of their final release.

VxWorks versions prior to 6.5 are not affected by the Urgent-11 vulnerabilities.

Impacted Product Versions

Product	Model	Versions	First Released	Embedded OS	Affected Component
Xprezzon	91393	v3.00.00 - 3.08.02	03/08/2011	VxWorks 6.6	Operating System
Qube	91390	v3.01.00 - 3.08.02	12/25/2012	VxWorks 6.6	Operating System
Qube Mini	91389	v3.07.00 - 3.08.02	04/21/2016	VxWorks 6.6	Operating System

Product	Model	Versions	First Released	Embedded OS	Affected Component
UVSL Monitors	91367, 91369, 91370, 91387	v2.03.00 - 2.03.13	10/29/2009	VxWorks 6.6	Operating System

3. VULNERABILITY IMPACTS

3.1 SCOPE

Geographic Regions Affected: Worldwide

Application/Product/Service Affected:

- VxWorks 6.9.4.11 and earlier are affected by one or more of these CVEs (see detail below)
- Older, End-of-Life versions of VxWorks back to 6.5 are also affected by one or more of these CVEs (see detail below)

3.2 TECHNICAL DETAILS

Information in the table below is provided by Wind River and identifies the security vulnerabilities that impact the IPNet communications stack. There are 11 specific exploits that could be applicable (CVEs – identified by their Common Vulnerability or Exposure ID). The table identifies operating system versions that are relevant to describing how these may impact Spacelabs PMC products, sorted in order of Common Vulnerability Scoring System (CVSS) severity.

CVE	Defect	Component	CVSS v3	Title	pre-Vx6.5	Vx 6.5	Vx 6.6	RCE
CVE-2019-12256	V7NET-2423	TCP/IP-stack	9.8	Stack overflow in the parsing of IPv4 packets' IP options	N	N	N	Y
CVE-2019-12257	VXW6-87101	DHCP Client	8.8	Heap overflow in DHCP Offer/ACK parsing inside	N	Y	Y	Y
CVE-2019-12255	VXW6-87100	TCP/IP-stack	9.8	TCP Urgent Pointer = 0 leads to integer underflow	N	Y	Y	Y
CVE-2019-12260	V7NET-2425	TCP/IP-stack	9.8	TCP Urgent Pointer state confusion caused by malformed	N	N	N	Y
CVE-2019-12261	V7NET-2425	TCP/IP-stack	8.8	TCP Urgent Pointer state confusion during connect() to	N	N	N	Y
CVE-2019-12263	V7NET-2425	TCP/IP-stack	8.1	TCP Urgent Pointer state confusion due to race condition	N	N	Y	Y
CVE-2019-12258	V7NET-2426	TCP/IP-stack	7.5	DoS of TCP connection via malformed TCP options	N	Y	Y	N
CVE-2019-12259	V7NET-2428	TCP/IP-stack	6.3	DoS via NULL dereference in IGMP parsing	N	Y	Y	N
CVE-2019-12262	V7NET-2427	TCP/IP-stack	7.1	Handling of unsolicited Reverse ARP replies (Logical Flaw)	N	Y	Y	N
CVE-2019-12264	V7NET-2428	DHCP Client	7.1	Logical flaw in IPv4 assignment by the ipdhcpc DHCP client	N	Y	Y	N
CVE-2019-12265	V7NET-2428	TCP/IP-stack	5.4	IGMP Information leak via IGMPv3 specific membership	N	Y	Y	N

Note: All of our affected products are in the Vx 6.6

The following is a summary of the impact of the Urgent-11 CVEs as they apply to the affected Spacelabs equipment:

1. Six of the vulnerabilities (CVE-2019-12256, CVE-2019-12255, CVE-2019-12260, CVE-2019-12261, CVE-2019-12263 and CVE-2019-12257) are classified as critical and enable Remote Code Execution (RCE).
    a. 3 of these (CVE-2019-12256, CVE-2019-12260 and CVE-2019-12261) do not apply as Spacelabs products use only VxWorks 6.6.
    b. CVE-2019-12263 does not apply as it requires the creation of a race condition between multiple threads and the Spacelabs products execute as a single CPU thread.
2. The remaining five vulnerabilities are classified as denial of service, information leaks or logical flaws.

3.3 SUMMARY OF OPERATIONAL IMPACTS

These vulnerabilities could be used to compromise a Spacelabs product in the following ways:

- Monitor Reset: The most likely risk from these vulnerabilities is that an attack could force the Spacelabs monitor to reboot. The monitor would automatically restart if it remains powered on (standard behavior). Alarm settings would persist and monitoring would resume after the system reset. This entire process (recovery and restart) would be completed within 30 seconds or less.

- Denial of Service: While less likely, it could be possible to create a cascade of monitor resets directed at the same monitor. This would result in loss of patient monitoring. This attack would be evident to the healthcare staff, and in response, the monitor could be taken off-line from the network to stop the attack. By being taken off-line there would be a loss of communication to centralized monitoring services such a central station or ICS, but local patient monitoring would continue at the device level.

- Remote Code Execution: In limited scenarios, it may be possible to craft an attack using one of the Urgent-11 vulnerabilities where the attacker can make different information appear on monitors than is accurate for the patient. This vulnerability creates the highest operational risk, but it would be a very complex attack to implement. The correct patient information remains on remote monitors, in ICS, and in the EHR.

Our analysis has shown that it is unlikely that an attack that makes use of the vulnerabilities would impact clinical use. To date, Spacelabs Healthcare has received no complaints involving clinical use that we have been able to associate with Urgent-11.

3.4 TECHNICAL DETAILS

The following is a breakdown of the specific CVEs and the technical details associated with these risks.

3.4.1 STACK-BASED BUFFER OVERFLOW CWE1-121 **[NOT APPLICABLE]**

CVE-2019-12256 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

This vulnerability does not apply to Vx 6.6, and therefore does not apply to affected Spacelabs Products.

3.4.2 HEAP-BASED BUFFER OVERFLOW CWE-122

CVE-2019-12257 has been assigned to this vulnerability. A CVSS v3 base score of 8.8 has been calculated; the CVSS vector string is (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

DHCP packets may go past the local area network (LAN) via DHCP-relays but are otherwise confined to the LAN.

The DHCP-client may be used by VxWorks and in the bootrom. Bootrom, using DHCP/BOOTP, is only vulnerable during the boot-process.

Potential impact with affected Spacelabs devices:

- As we use the affected DCHP-client code in the patient monitors these devices are vulnerable to this attack.
- The most likely result of an attempt to exploit this vulnerability would be that the monitor resets and then resumes normal monitoring.
- In the worst case, this vulnerability can potentially lead to remote code execution (RCE).
    - This can be mitigated if the healthcare organization has a firewall configuration that provides security to our products, but it is not clear if this can be relied on in all situations.
    - See separate section regarding the potential outcomes of remote code execution on the affected Spacelabs devices.
- Turning off the use of DHCP in the monitor's network setup does ***not*** mitigate this vulnerability.

3.4.3 INTEGER UNDERFLOW (WRAP OR WRAPAROUND) CWE-191

CVE-2019-12255 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

An attacker can either hijack an existing TCP-session and inject bad TCP-segments or establish a new TCP-session on any TCP-port listened to by the target.

This vulnerability could lead to a buffer overflow of up to a full TCP receive-window.

Potential impact with affected Spacelabs devices:

- The monitors are vulnerable to the attack as evidenced by Armis' use of this attack vector in their demonstration video.
- The most likely result of an attempt to exploit this vulnerability would be that the

[1] CWE = Common Weakness Enumeration. It is a standard way of classifying and identifying the element that a vulnerability may affect. More information can be obtained here: https://cwe.mitre.org/about/

monitor resets and then resumes normal monitoring.
- In the worst case, this vulnerability can potentially lead to remote code execution (RCE).
  - Per the Wind River security advisory, if the affected devices reside behind a firewall, this vulnerability can be mitigated via the firewall, but it is not clear if this can be relied on in all situations.
  - See separate section regarding the potential outcomes of remote code execution on the affected Spacelabs devices.

3.4.4 IMPROPER RESTRICTION OF OPERATIONS WITHIN THE BOUNDS OF A MEMORY BUFFER CWE-119 **[NOT APPLICABLE]**

CVE-2019-12260 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

This vulnerability does not apply to Vx 6.6, and therefore does not apply to affected Spacelabs Products.

3.4.5 IMPROPER RESTRICTION OF OPERATIONS WITHIN THE BOUNDS OF A MEMORY BUFFER CWE-119 **[NOT APPLICABLE]**

CVE-2019-12261 has been assigned to this vulnerability. A CVSS v3 base score of 8.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H).

This vulnerability does not apply to Vx 6.6, and therefore does not apply to affected Spacelabs Products.

3.4.6 CONCURRENT EXECUTION USING SHARED RESOURCE WITH IMPROPER SYNCHRONIZATION ('RACE CONDITION') CWE-362 **[NOT APPLICABLE]**

CVE-2019-12263 has been assigned to this vulnerability. A CVSS v3 base score of 8.1 has been calculated; the CVSS vector string is (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).

This vulnerability relies on a race-condition that is not possible to create in a single threaded process as the Spacelabs monitors have been designed.
- As the Spacelabs monitor code executes in a single CPU-thread (kernel) mode this vulnerability (the risk of concurrent execution) does not apply.

3.4.7 ARGUMENT INJECTION OR MODIFICATION CWE-88

CVE-2019-12258 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

An attacker with the source and destination TCP-port and IP-addresses of a session can inject invalid TCP-segments into the flow, causing the TCP-session to be reset.

The most likely outcome is a crash of the application reading from the affected socket.

Potential impact with affected Spacelabs devices:

- The most likely result of an attempt to exploit this vulnerability would be that the monitor resets and then resumes normal monitoring.

3.4.8. NULL POINTER DEREFERENCE CWE-476 **[NOT APPLICABLE]**

CVE-2019-12259 has been assigned to this vulnerability. A CVSS v3 base score of 6.3 has been calculated; the CVSS vector string is (AV:A/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H).

This vulnerability requires that at least one IPv4 multicast address has been assigned to the target in an incorrect way (e.g., using the API intended for assigning unicast-addresses).

- An attacker must first use CVE-2019-12264 to incorrectly assign a multicast IP-address.
- Then an attacker on the same LAN as the target system may use vulnerability CVE-2019-12259 to cause a NULL-pointer reference, which most likely will crash the task.
- The Spacelabs devices are not vulnerable to this exploit.

3.4.9. ARGUMENT INJECTION OR MODIFICATION CWE-88

CVE-2019-12262 has been assigned to this vulnerability. A CVSS v3 base score of 7.1 has been calculated; the CVSS vector string is (AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H).

An attacker residing on the LAN can send reverse-ARP responses to the victim system to assign unicast IPv4 addresses to the target.

Potential impact with affected Spacelabs devices:

- The Spacelabs devices are vulnerable to this exploit.
- Per the Wind River security advisory the action will not cause any direct harm other than increased usage of RAM. However, the vulnerability may indirectly cause network connectivity issues for the system on the LAN if the assigned IP-addresses collide with other devices on the LAN.
- If an attack resulted in a network address conflict the network infrastructure (routers, switches, etc.) may block network to / from the affected devices.

3.4.10 ARGUMENT INJECTION OR MODIFICATION CWE-88

CVE-2019-12264 has been assigned to this vulnerability. A CVSS v3 base score of 7.1 has been calculated; the CVSS vector string is (AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H).

An attacker residing on the LAN may choose to hijack a DHCP-client session that requests an IPv4 address. The attacker can send a multicast IP-address in the DHCP offer/ack message, which the victim system then incorrectly assigns.

This vulnerability can be combined with CVE-2019-12259 to create a denial-of-service condition.

Potential impact with affected Spacelabs devices:

- The Spacelabs devices are technically vulnerable to this exploit.
- However, per the Wind River security advisory, this exploit is not useful in isolation and only has the potential to be disruptive when combined with CVE-2019-12259 to which the Spacelabs devices are not vulnerable.

3.4.11 ARGUMENT INJECTION OR MODIFICATION CWE-88

CVE-2019-12265 has been assigned to this vulnerability. A CVSS v3 base score of 5.4 has been calculated; the CVSS vector string is (AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).

Potential impact with affected Spacelabs devices:

- The Spacelabs devices are vulnerable to this exploit.
- Per the Wind River security advisory, attacks against link local multicast addresses allow an attacker on the LAN to make the victim system transmit data to the network that has not been properly set. Specifically, the data transmitted from the network might be information from packets previously received/sent by the network stack.

4. RECOMMENDED MITIGATIONS AND REMEDIATIONS

Spacelabs Healthcare is developing specific patches for each of our impacted products. Existing customers can sign up at the Spacelabs customer portal for access to our latest patches at (http://www.spacelabshealthcare.com/products/security/). We expect to release the patch for our current products by the end of October 2019. The patch for our older UVSL products that are affected will be released shortly thereafter.

If you need help in identifying the Spacelabs products that are impacted, contact Spacelabs Technical Support at 800-522-7025, option 2.

It is possible to block the potential for attacks that use these vulnerabilities via firewall rules that filter specific network traffic. Updated and monitored hospital firewalls can mitigate many of the attack vectors and thus not allow the Spacelabs devices to become compromised.

The enterprise security firm Armis has posted a report on its website listing a number of mitigations that can be put in place. Please see https://armis.com/urgent11/.

More information:
Spacelabs is publishing a more in-depth technical advisory of the analysis of these vulnerabilities at the ICS-CERT website (www.us-cert.gov/ics). This report is being published under TPS protocol and can be accessed via validated medical device owners at the CISA ICS-CERT site (https://www.us-cert.gov/ics).

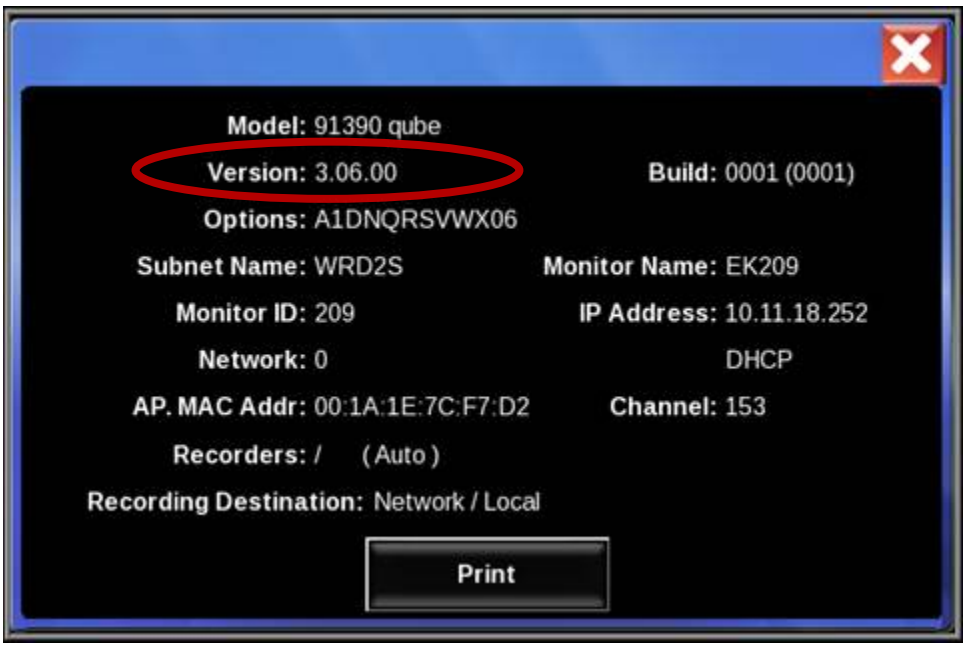
This information is available to registered users of the Spacelabs Cybersecurity Portal (http://www.spacelabshealthcare.com/products/security/). Please refer to these sites for the latest information on identified threats and Spacelabs product mitigations.

4.1 DETECTION

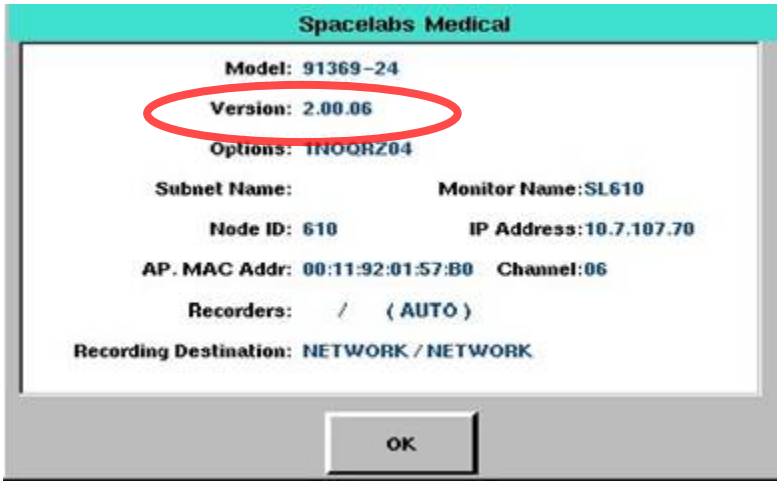
The customer can determine if they have product/versions that are affected by manually checking the devices. Below are the steps on how to check software version(s) on a device.

- Double click “HELP ?” key on the monitor screen to obtain the software version of the device.

- Xprezzon (91393), Qube (91390) and Qube mini (91389) will appear with a pop up window as shown below:



- UVSL (91367, 91369, 91370 and 91387) will appear with a pop up window as shown below:



If an organization is running advanced intrusion detection tools like SNORT (link here) they could use the following rules to verify product vulnerability:

The most severe URGENT/11 vulnerabilities abuse esoteric parts of the TCP/IP stack that are almost never used by legitimate applications. Armis has developed the following Snort rules to be freely used by Firewall and IDS solutions to detect and prevent any attempt to exploit these vulnerabilities:

1. Detection of any use of the Urgent pointer can be done with the following Snort rule. Be advised that this rule might cause some false positives in the very rare case when Urgent Pointer is used by a legitimate application (such as the ancient RLOGIN protocol)

   alert tcp any any -> any any (flags: U+; msg: "OS-VXWORKS - Use of Urgent Flag might indicate potential attempt to exploit an Urgent11 RCE vulnerability"; classtype:attempted-admin; reference:cve,2019-12255; reference:cve,2019-12260; reference:cve,2019-12261; reference:cve,2019-12263; reference:url,armis.com/urgent11; rev: 1; sid:1000002)

2. Detection of packets that contain both SYN, URG and FIN flags. This combination will never occur in legitimate TCP traffic, and is a strong indication of potential exploit attempt of URGENT/11:

   alert tcp any any -> any any (flags: SUF+; msg: "OS-VXWORKS Illegal use of Urgent pointer - Potential attempt to exploit an Urgent11 RCE vulnerability"; classtype:attempted-admin; reference:cve,2019-12255; reference:cve,2019-12260; reference:cve,2019-12261; reference:cve,2019-12263; reference:url,armis.com/urgent11; rev: 1; sid:1000001)

3. Detection of any IP packet that contains the LSRR or SSRR options. These options should never be used in modern networks, regardless of the potential RCE vulnerability they present to VxWorks devices. Most firewalls will drop any IP packet that contain these packets for security reasons, and IDS solutions can detect any use of such packets using the following Snort rules:

   alert ip any any -> any any (ipopts: lsrr; msg: "OS-VXWORKS Use of LSRR option, potential attempt to exploit an Urgent11 RCE vulnerability"; reference:cve,2019-12256; classtype:attempted-admin; reference:url,armis.com/urgent11; rev: 1; sid:1000003)
   alert ip any any -> any any (ipopts: ssrr; msg: "OS-VXWORKS Use of SSRR option, potential attempt to exploit an Urgent11 RCE vulnerability"; reference:cve,2019-12256; classtype:attempted-admin; reference:url,armis.com/urgent11; rev: 1; sid:1000004)

4.2 SHORT TERM MITIGATION ACTIONS

Customer firewalls should be secured and configured to block appropriate traffic.

The enterprise security firm Armis has posted a report on its website listing a number of mitigations that can be put in place. Please see https://armis.com/urgent11/.

4.3 REMEDIATION PLANS

Spacelabs will provide software patches for all affected devices.

a) Customers with affected product under manufacturer's warranty or an active Service Support Agreement:
   1) Contact Spacelabs Service (800-522-7025, option 1 (dispatch FSE)) to schedule an upgrade on your affected devices with your field service engineer
   2) If scheduling does not meet the customer's request, a software patch can be alternatively provided to the customer for self-installation by the Biomed department. A CSN will be created by Spacelabs that instructs Biomeds how to install software appropriately.
b) Customers with affected devices that are not covered under a manufacturer's warranty or service support agreement:
   1) The upgrade instruction (CSN) will be provided to the customer for self-installation – free of charge.
   2) If the customer would like Spacelabs to upgrade the affected devices, standard service rate will apply for labor and travel.
c) Depending on software version that a customer is changing from may require Clinical Education Training.
   1) Scheduling for clinical training will need to take place between Spacelabs' Clinical Educator and the customer. Standard charges will apply.
   2) Clinical staff may consider making a training video that offsets this training that needs to take place (this is to be determined).
   3) It has been identified that Xprezzons, Qubes and Qube Minis, software versions prior to 3.06 will require Clinical Education Training. The UVSL devices (91367, 91369, 91370 and 91387) with software versions prior to 2.03.13 will require Clinical Education Training.

5. ADDITIONAL INFORMATION

Spacelabs has adopted a cybersecurity program that is based on National Institute of Standards and Technology's 800-53 requirements. We continually analyze our products for vulnerabilities and weaknesses in collaboration with customers, regulatory agencies, and external experts to maintain and improve the security of our products. You will find the latest cybersecurity information on our website at https://www.spacelabshealthcare.com/products/security/.

If you have any questions about this Security Advisory, please contact Spacelabs at 1-800-522-7025 and select 2 for Technical Support.

In addition, general inquiries can be submitted using the Contact Us form on our website.

5.1 DOCUMENT HISTORY

Version	Release Date	Purpose
Rev. A	10 October 2019	Initial Release

6. TERMS OF USE

The information in this document is subject to change without notice. In no event will Spacelabs or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages

of any nature or kind arising from the use of this document, even if Spacelabs or its suppliers have been advised of the possibility of such damages.

This document contains confidential and proprietary language and may not be reproduced or shared with a third party without written permission from Spacelabs. All rights to registrations and trademarks reside with their respective owners.