SPACELABS
HEALTHCARE

# Security Advisory

## "BadAlloc" Vulnerability Assessment and Potential Product Impact Statement

| Ref Doc ID | Version | Release Date | Advisory Status | Related CVE(s) | Operational Risk |
|---|---|---|---|---|---|
| 079-0242-00 | B | 4 June 2021 | ACTIVE | See ICS Advisory (ICSA-21-119-04) for details. | Low |

### 1. VULNERABILITY

Spacelabs Healthcare has been made aware of recently published vulnerabilities collectively known as "BadAlloc" that details vulnerabilities found in multiple Real-Time Operating Systems (RTOS) and supporting libraries. Cybersecurity & Infrastructure Security Agency (CISA) issued an advisory to provide notice of the reported vulnerabilities and identify baseline mitigations for reducing risks to these and other cybersecurity attacks.

The 23 vulnerabilities identified across 25 RTOS by the security researchers from Microsoft research groups reported that successful exploitation of these vulnerabilities could result in unexpected behavior such as a crash or a remote code injection/execution.

Spacelabs has conducted an assessment to identify the potential impact on our products. Our assessment has found that Spacelabs Patient monitors including Qube, Qube Mini, Xprezzon, and UVSL Monitors are impacted by one of the identified vulnerabilities.

Spacelabs utilizes Wind River VxWorks that was identified as one of the RTOS affected by BadAlloc for the Patient Monitors. More details can be found on Wind River's website; links are available in the reference section.

**Security Impact:**

| Security Impact | Notes |
|---|---|
| Availability | **Technical Impact:** *DoS: Crash, Exit, or Restart; DoS: Resource Consumption (CPU); DoS: Resource Consumption (Memory); DoS: Instability* |
| Integrity | **Technical Impact:** *Modify Memory* |
| Confidentiality | **Technical Impact:** *Execute Unauthorized Code or Commands; Bypass Protection Mechanism* |

## 2. OPERATIONAL RISK ASSESSMENT SUMMARY

Spacelabs considers the operational risk to its devices from a BadAlloc attack to be low. In our review there is only a limited chance that a device could be compromised due to the fact that a properly configured firewall in the hospital network would mitigate the likelihood of an attack from outside the organization and since remote code execution would require that a bad actor already be positioned within the hospital network as a result of a prior attack.

Common hospital protocol involves the use of multiple parameters and physical assessment of patients in determining treatment. For this reason, in the event that a Spacelabs monitor is compromised due to an attack exploiting BadAlloc vulnerabilities there is less likelihood of incorrect treatment. There are also typically redundant alarm systems in place to decrease the likelihood of delay in treatment.

Spacelabs is working with the vendor to develop software patches that will be available to keep an attack from using the identified operating system vulnerabilities. In the meantime, customers are encouraged to ensure their facility maintains a secure network firewall to protect its products and data.

## 3. RECOMMENDATIONS

Spacelabs recommends the following defenses and mitigations be applied to the enterprise environment.

- Minimize network exposure for all patient monitoring devices such as monitors (Qube, Qube mini, Xprezzon and UVSL) with the use of network segmentation, placement of these devices behind hospital firewalls, and ensuring that they are not accessible from the Internet.
- Block suspicious external IP addresses at the hospital firewalls. Monitor traffic internally for unusual behavior.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its connected devices.
- Implement defense-in-depth within the enterprise environment consisting of tools such as Intrusion Detection/Prevention Systems (IDS/IPS), firewalls, and network access control (NAC).
- Implement and maintain an anti-malware solution (also called “anti-virus”) and an endpoint detection and response (EDR) solution.
- Disable remote access services and protocols such as Remote Desktop Protocol (RDP) unless needed. Monitor and restrict remote access usage on a least-privilege basis.
- Have backup and restore processes and procedures in place for disaster recovery and incident response.
- Monitor and maintain account provisioning and access control based on the principle of least privilege.

SPACELABS
HEALTHCARE

## 4. EXAMINATION OF SPACELABS PRODUCTS

### ASSESSMENT OF SPACELABS PRODUCTS

In response to the publication of these vulnerabilities, Spacelabs has conducted an assessment to identify devices potentially at risk to this set of vulnerabilities. Please note information is subject to change as the situation evolves.

**Patient Monitoring and Connectivity Products**

| Product | Host Operating System | Impact Assessment |
|---|---|---|
| XprezzNet 96190 | Windows Server 2012 R2, Windows Server 2016 | Not impacted. |
| Intesys Clinical Suite (ICS) | Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 | Not impacted. |
| Xhibit Telemetry Receiver (XTR) 96280 | Windows Embedded Standard 7 SP1 | Not impacted. |
| Xhibit 96102 / XC4 96501 | Windows Embedded Standard 7 SP1 | Not impacted. |
| **Bedside Monitors**<br>• Xprezzon 91393<br>• Qube 91390<br>• Qube Mini 91389<br>• Ultraview SL 91367, 91369, 91370, and 91387 | VxWorks 6.6 | Impacted. There is currently no patch for the version of VxWorks running in the monitors. Spacelabs will work with RTOS developers and will issue a revision to this document when the patch is available. |

**Diagnostic Cardiology Products**

| Product | Host Operating System | Impact Assessment |
|---|---|---|
| Sentinel | Windows 7 & 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 | Not impacted. |
| Pathfinder SL | Windows 7, Windows 10 | Not impacted. |
| Lifescreen Pro | Windows 10 | Not impacted. |
| Lifecard CF | No OS | Not impacted. |
| EVO | No OS | Not impacted. |
| Eclipse Pro | No OS | Not impacted |
| CardioExpress SL6A / SL12A | Embedded OS (uC/OS II V2.84) | Pending Review. |
| CardioExpress SL18A | Embedded OS (Linux Kernel 2.6.35.3) | Not impacted. |

| Product | Host Operating System | Impact Assessment |
|---|---|---|
| **ABP**<br>• OnTrak<br>• 90217A<br>• 90207 | No OS | Not impacted. |

**Safe N Sound**

| Product | Host Operating System | Impact Assessment |
|---|---|---|
| Spacelabs Cloud | Varies | Not impacted. |
| SafeNSound | Not applicable | Not impacted. |

## 5. Additional Resources

- Microsoft Security Response Center - https://msrc-blog.microsoft.com/2021/04/29/badalloc-memory-allocation-vulnerabilities-could-affect-wide-range-of-iot-and-ot-devices-in-industrial-medical-and-enterprise-networks/
- CISA ICS Advisory ICSA-21-119-04 - https://us-cert.cisa.gov/ics/advisories/icsa-21-119-04
- Wind River - https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2020-28895
- Wind River (permission required): https://support2.windriver.com/index.php?page=defects&on=view&id=V7LIBC-1327
- Spacelabs Patch Qualification Customer Portal - https://www.spacelabshealthcare.com/products/security/patch-test-reports-access-form/?redirect_to=%2Fproducts%2Fsecurity%2Fpatch-test-reports%2F

## 6. Document History

| Version | Release Date | Purpose |
|---|---|---|
| Rev B | 4 June 2021 | BadAlloc Vulnerability Assessment and Potential Product Impact Statement |

## 7. 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.