SPACELABS HEALTHCARE

Security Advisory

CrowdStrike Vulnerability Assessment and Potential Product Impact Statement

Ref Doc ID	Version	Release Date	Advisory Status	Related CVE(s)
079-0274-00	A	<2024-08-09>	ACTIVE	N/A

1. VULNERABILITY OVERVIEW

Spacelabs Healthcare has been made aware of a third-party issue with a CrowdStrike content configuration update on July 19, 2024, on Windows hosts running CrowdStrike sensor version 7.11 and above that were online during the initial update release. Please note this is not a Spacelabs product but may be used by customers to manage connectivity across various products/platforms.

2. RISK ASSESSMENT SUMMARY

Spacelabs has conducted an assessment to identify the potential impact of CrowdStrike vulnerability on our products. Our assessment has found that no Spacelabs products are directly affected by this vulnerability.

As Spacelabs continue to gain a deeper understanding of the impact of this vulnerability, we will continue to publish technical information to help customers detect, investigate, and mitigate the vulnerability across all our products where applicable.

3. RECOMMENDATIONS

Spacelabs recommends the following:

- Customers in the United States may contact Technical Support to schedule their SW upgrade to the current General Release version.
    - Phone: (+1) 800-522-7025
    - Email: support@spacelabs.com
- Customers in Canada may contact Canada Technical Support to schedule their SW upgrade to the current General Release version.
    - Phone: (+1) 905 564 2229
    - Email: canada.service@spacelabs.com
- International customers may contact Global Technical Support to schedule their SW upgrade to the current General Release version.
    - Phone: (+44) 1992 507 740
    - Email: emea.service@spacelabs.com

GENERAL SECURITY RECOMMENDATIONS

- Minimize network exposure for all products 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.
- Enable multi-factor authentication where possible.
- Block suspicious external IP addresses at the enterprise firewalls. Monitor traffic internally for unusual behavior.
- Implement defense-in-depth within the enterprise environment consisting of tools such as intrusion detection systems/intrusion 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.
- Apply applicable patches, hotfixes, and updates to servers and products when available and after they have been validated.

4. EXAMINATION OF SPACELABS PRODUCTS

4.1 ASSESSMENT OF SPACELABS PRODUCTS

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

Patient Monitoring and Connectivity (PMC) Products

PRODUCT	OPERATING SYSTEM	IMPACT ASSESSMENT
XprezzNet 96190	Windows Server 2012 R2 Windows Server 2016 Windows Server 2019	Not impacted

PRODUCT	OPERATING SYSTEM	IMPACT ASSESSMENT
Intesys Clinical Suite (ICS)	Windows Server 2012 R2 Windows Server 2016 Windows Server 2019	Not impacted
Intesys Clinical Suite (ICS) Clinical Access Workstations	Windows 10 Windows 11 Windows 2016 Windows 2019	Not impacted
Xhibit Telemetry Receiver (XTR) 96280	Windows 10 IoT Enterprise Version 1809	Not impacted
Xhibit 96102 / XC4 96501	Windows 10 IoT Enterprise Version 1809	Not impacted
Bedside Monitors • Xprezzon 91393 • Qube 91390 • Qube Mini 91389	VxWorks 6.9	Not impacted
DM3, DM4 Monitor	Windows CE	Not impacted

Diagnostic Cardiology (DC) Products

PRODUCT	OPERATING SYSTEM	IMPACT ASSESSMENT
Sentinel	Windows 10 Windows 11 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019	Not impacted
Pathfinder SL	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
Eclipse Mini	No OS	Not impacted
CardioExpress SL6A / SL12A	Embedded OS (uC/OS II V2.84)	Not impacted
CardioExpress SL18A	Embedded OS (Linux Kernel 2.6.35.3)	Not impacted

PRODUCT	OPERATING SYSTEM	IMPACT ASSESSMENT
ABP • OnTrak • 90217A • 90207	No OS	Not impacted

SafeNSound (SNS)

PRODUCT	OPERATING SYSTEM	IMPACT ASSESSMENT
Spacelabs Cloud	Varies	Not impacted
SafeNSound	Not applicable	Not impacted
SafeNSound desktop		Not impacted
SafeNSound mobile		Not impacted

Rothman Index (RI)

PRODUCT	OPERATING SYSTEM	IMPACT ASSESSMENT
Spacelabs Cloud	Varies	Not impacted
Rothman Index	Not applicable	Not impacted
Rothman Index mobile		Not impacted

SPACELABS HEALTHCARE

5. Additional Resources

#	RESOURCE	URL
1	CISA Article	Widespread IT Outage Due to CrowdStrike Update | CISA
2	CrowdStrike Remediation and Guidance Hub	Falcon Content Update Remediation and Guidance Hub | CrowdStrike

6. Document History

Version	Release Date	Purpose
Rev A	2024-08-09	CrowdStrike 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.