SPACELABS HEALTHCARE

Security Advisory

Windows Kernel Elevation of Privilege Vulnerability Assessment and Potential Product Impact Statement

Ref Doc ID	Version	Release Date	Advisory Status	Related CVE(s)
079-0292-00	A	<2025-11-24>	ACTIVE	CVE-2025-62215

1. VULNERABILITY OVERVIEW

Spacelabs Healthcare has been made aware of a recently published Windows Kernel elevation of privilege vulnerability to impact on Windows 10 products. This vulnerability stems from concurrent execution of code that uses a shared resource without proper synchronization known as race condition in Windows Kernel allowing authorized attackers to elevate privileges locally.

2. RISK ASSESSMENT SUMMARY

Spacelabs has conducted an assessment to identify the potential impact of the Windows Kernel elevation of privilege vulnerability on our products. Our assessment has found that Spacelabs Xhibit SW v1.5.0 to the latest v1.6.1 and XTR SW v1.4.0 to the latest v1.4.2 all running on Windows 10 1809 are affected by this vulnerability.

Spacelabs has assessed the potential impact of this vulnerability on the Xhibit and XTR product. We have concluded that since the system operates with a single user account possessing administrator privileges, meaning the vulnerability cannot further elevate privileges beyond what is already granted then this vulnerability does not increase risk.

Spacelabs has also identified that ICS Clinical Access workstations, as well as the Sentinel, Pathfinder, and Lifescreen Pro applications hosted on Windows 10 systems, are impacted by the security vulnerability. Immediate remediation is required to maintain system integrity and safeguard sensitive clinical data.

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

FOR WINDOWS 10 WORKSTATIONS

- Apply the latest Windows 10 security updates to all affected systems.
- Verify that ICS Clinical Access, Sentinel, Pathfinder, and Lifescreen Pro applications are functioning correctly after patch installation.

SPACELABS HEALTHCARE

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 2019 Windows Server 2022	Not impacted
Intesys Clinical Suite (ICS)	Windows Server 2019 Windows Server 2022	Not impacted
Intesys Clinical Suite (ICS) Clinical Access Workstations	Windows 10 Windows 11 Windows 2016 Windows 2019	Impacted
Xhibit Telemetry Receiver (XTR) 96280	Windows 10 IoT Enterprise Version 1809	Impacted
Xhibit 96102 / XC4 96501	Windows 10 IoT Enterprise Version 1809	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 2016 Windows Server 2019	Impacted
Pathfinder SL	Windows 10	Impacted
Lifescreen Pro	Windows 10	Impacted
Lifecard CF	No OS	Not impacted

PRODUCT	OPERATING SYSTEM	IMPACT ASSESSMENT
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
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	CVE-2025-62215 Detail	CVE-2025-62215
2	CISA Article	CISA Adds Three Known Exploited Vulnerabilities to Catalog
3	Microsoft Security Updates	CVE-2025-62215 Security Vulnerability

6. Document History

Version	Release Date	Purpose
Rev A	11-24-2025	Windows Kernel elevation of privilege 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.