SPACELABS HEALTHCARE

# Security Advisory

## Sentinel version 10.5.x and 11.x.x Vulnerability Assessment and Potential Product Impact Statement

| Ref Doc ID | Version | Release Date | Advisory Status | Related CVE(s) |
|---|---|---|---|---|
| 079-0273-00 | A | <2026-05-29> | ACTIVE | 2026-0611 |

### 1. VULNERABILITY OVERVIEW

Spacelabs Healthcare has been made aware of an unauthenticated remote code execution vulnerability through a deprecated .NET Remoting HTTP channel on port 8989. The vulnerability allows attackers to perform arbitrary file read and write operations by supplying valid .NET URI endpoints to achieve unauthenticated remote code execution on the system.

### 2. RISK ASSESSMENT SUMMARY

Spacelabs has conducted an assessment to identify the potential impact of the Unauthenticated RCE via .NET Remoting vulnerability on our products. Our assessment has found that Spacelabs Sentinel is affected by this vulnerability.

Spacelabs has assessed the potential impact of this vulnerability on the Sentinel product. We have concluded that Sentinel v10.5.x and higher (v11.x.x) are vulnerable to this exploit, which does impact Confidentiality, Integrity and Availability of the Sentinel Software.

Spacelabs is reporting both the CVSS Scores for the unmitigated vulnerability and the mitigated vulnerability.

Unmitigated 11.6.0 Unauthenticated RCE via .NET Remoting
CVSS Score 9.2
CVSS Vector String: 4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Mitigated 11.6.0 Unauthenticated RCE via .NET Remoting
CVSS Score: 2.3
CVSS Vector String: 4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N

This is based on the input from VulnCheck as implemented and described by GM SecTec with Spacelabs verification and ability to reproduce the exploit as reported. Spacelabs would like to recognize VulnCheck and GM SecTec for their collaboration and contribution to the report.

### 3. RECOMMENDATIONS

Update the version of Sentinel Software to the latest v11.6.2. This version has implemented the correction for the .NET software that was used in the proof of concept exploit as reported by GM SecTec and VulnCheck.

SPACELABS HEALTHCARE

Minimize network exposure for all Sentinel versions by placement of these systems ensuring that they are not accessible from the Internet, behind hospital firewalls and the segmentation of internal networks and specifically

- Block port 8989 for all network communications which is required for the exploit. This port is not used by the Sentinel application by default. The MS Windows Defender Firewall blocks this port by default, which mitigates vulnerability. This has been tested and verified by GM SecTec and Spacelabs.

- US customers may reach out to Technical Support to schedule their Sentinel Software update or upgrade to v11.6.2.
  - Phone: (+1) 800-522-7025
  - Email: support@spacelabs.com

- Canada customers may reach out to Canada Technical Support to schedule their Sentinel Software update or upgrade to v11.6.2.
  - Phone: (+1) 905 564 2229
  - Email: SLCanadaCustomerService@spacelabs.com

- International customers may reach out to Global Technical Support to schedule their Sentinel Software update or upgrade to v11.6.2.
  - Phone: (+44) 1992 507 740
  - Email: GTSDC@spacelabs.com

**GENERAL SECURITY RECOMMENDATIONS**

- 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.

**Diagnostic Cardiology (DC) Products**

| PRODUCT | OPERATING SYSTEM | IMPACT ASSESSMENT |
|---|---|---|
| Sentinel | Windows 10<br>Windows 11<br>Windows Server 2019<br>Windows Server 2022 | Impacted |

SPACELABS HEALTHCARE

## 5. Additional Resources

| # | RESOURCE | URL |
|---|---|---|
| 1 | CVE-2026-0611 Detail | https://www.cve.org/CVERecord?id=CVE-2026-0611 |
| 2 | VulnCheck Notification | https://www.vulncheck.com/advisories/spacelabs-healthcare-sentinel-unauthenticated-rce-via-net-remoting |

## 6. Document History

| Version | Release Date | Purpose |
|---|---|---|
| Rev A | 29 May 2026 | Sentinel .NET Remoting 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.