SPACELABS HEALTHCARE

Security Advisory

Code injection attacks using publicly disclosed ASP.NET machine keys Vulnerability Assessment and Potential Product Impact Statement

Ref Doc ID	Version	Release Date	Advisory Status	Related CVE(s)
079-0266-00	A	2025-02-27	ACTIVE	CVE-2020-0688, CVE-2023-32312, CVE-2023-33170, CVE-2023-35391, CVE-2023-36038, CVE-2023-36558, CVE-2023-36560, CVE-2023-36899, CVE-2023-37267, CVE-2023-38694, CVE-2023-41890, CVE-2023-48003, CVE-2023-48227, CVE-2023-48313, CVE-2023-49089, CVE-2023-49273, CVE-2023-49274, CVE-2023-49278, CVE-2023-49279, CVE-2023-49289, CVE-2024-10125, CVE-2024-28868, CVE-2024-29035, CVE-2024-34071, CVE-2024-35218, CVE-2024-39694, CVE-2024-40502, CVE-2024-43376, CVE-2024-43377, CVE-2024-49755, CVE-2024-49755, CVE-2024-55969, CVE-2024-55970

1. VULNERABILITY OVERVIEW

Spacelabs are aware of recent communication from Microsoft regarding publicly disclosed ASP.NET machine keys that could in certain circumstances be used to enable a ViewState code injection attack

2. RISK ASSESSMENT SUMMARY

Spacelabs has conducted an assessment to identify the potential impact of this vulnerability on our products.

Our assessment has found that Spacelabs XprezzNet software (V1.3.x and later) utilizes ASP .NET. Additionally, Sentinel software (V11.5.x and earlier) includes a configuration file that contains a publicly disclosed key. However, both Sentinel and XprezzNet do **not** make use of the ASP.NET ViewState feature, so are **not** impacted by this vulnerability.

No other Spacelabs products utilize ASP.NET and are not impacted by this vulnerability.

3. RECOMMENDATIONS

Tools such as Microsoft Defender for Endpoint may generate an “Publicly disclosed ASP.NET machine key“ alert indicating the presence of the publicly disclosed machine key

SPACELABS HEALTHCARE

The following Sentinel files

1. \inetpub\wwwroot\Sentinel\Bin\Spacelabs.Lomond.WebPortal.dll.config
2. \inetpub\wwwroot\Sentinel\Web.config

contain the following machine key entry.:

```
<machineKey validationKey=
"C7E18A68258395964BFE2A78B9F90F812186E43F1D70D014F3398E7E9E8D092E78E4F
753C935F45CAE77B52FA91AFCCA9A2FE55FC06307940229E702D3314610"
decryptionKey="48A617BD599AC6B42CD2CE59E58901DB0B6F811D0302A0C9"/>
```

These files may safely be **modified** to remove this machine key. This will not have an impact on the operation of Sentinel.

> **Warning: Do not delete these files or make any modifications other than to remove the machine key as this will render Sentinel inoperable.**

For additional questions or concerns:

- Customers in the United States may contact Technical Support.
  - Phone: (+1) 800-522-7025
  - Email: support@spacelabs.com
- Customers in Canada may contact Canada Technical Support.
  - Phone: (+1) 905 564 2229
  - Email: canada.service@spacelabs.com
- International customers may contact Global Technical Support.
  - 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 ensure 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.
- Have backup and restore processes and procedures in place for disaster recovery and incident response.

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 (V1.3.x and later)	Windows Server 2016 Windows Server 2019	Utilizes ASP .NET but no security impact.
Intesys Clinical Suite (ICS)	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 (V11.5.x and earlier)	Windows 10 Windows 11 Windows Server 2016 Windows Server 2019 Windows Server 2022	Disclosed keys are present within a configuration file but have no security impact.
Sentinel (V11.6)	Windows 10 Windows 11 Windows Server 2016 Windows Server 2019	Not Impacted

PRODUCT	OPERATING SYSTEM	IMPACT ASSESSMENT
	Windows Server 2022	
Pathfinder SL	Windows 10 Windows11	Not Impacted
Lifescreen Pro	Windows 10 Windows 11	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
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	Microsoft	https://www.microsoft.com/en-us/security/blog/2025/02/06/code-injection-attacks-using-publicly-disclosed-asp-net-machine-keys/
2	Zero Day Initiative	https://www.zerodayinitiative.com/blog/2020/2/24/cve-2020-0688-remote-code-execution-on-microsoft-exchange-server-through-fixed-cryptographic-keys

6. Document History

Version	Release Date	Purpose
Rev A	2025-02-27	Code injection attacks using publicly disclosed ASP.NET machine keys 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.