SPACELABS HEALTHCARE

Security Advisory

AMNESIA:33 Vulnerability Assessment and Potential Product Impact Statement

Ref Doc ID	Version	Release Date	Advisory Status	Related CVE(s)	Operational Risk
079-0238-00	A	December 15, 2020	ACTIVE	See ICS Advisory (ICSA-20-343-01) for details.	Low

1. VULNERABILITY

Spacelabs Healthcare has been made aware of recently published vulnerabilities collectively called AMNESIA:33, which impacts many embedded, Internet-of-Things (IoT) and IT devices. These vulnerabilities impact the underlying network drivers, or "stacks," that these devices use to connect to a network. Spacelabs has conducted an assessment to identify the potential impact on our products. Our assessment has found that no Spacelabs products are impacted by these vulnerabilities.

The set of 33 vulnerabilities identified by the security company Forescout impact devices used in many industries and across device domains, potentially including medical devices. The vulnerabilities impact several open-source TCP/IP stacks. Exploitation of the vulnerabilities can allow for DNS cache poisoning, remote code execution, denial of service of device network functionality, among other attack vectors.

2. RECOMMENDATIONS

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

- Train employees on social engineering and phishing techniques. Have a policy or process in place to report suspicious emails to the appropriate event and incident responders.
- Apply applicable patches, hotfixes, and updates to servers and products when available and after they have been validated.
- 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.
- Block suspicious external IP addresses at the enterprise firewalls. Monitor traffic internally for unusual behavior.

SPACELABS HEALTHCARE

3. EXAMINATION OF SPACELABS PRODUCTS

3.1 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	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 • Xprezzon 91393 • Qube 91390 • Ultraview SL	VxWorks 6.6	Not impacted.

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.
CardioExpress SL6A / SL12A	Embedded OS (uC/OS II)	Not impacted.
CardioExpress SL18A	Embedded OS (Linux)	Not impacted.
ABP • OnTrak • 90217A • 90207	No OS	Not impacted.

Safe N Sound

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

4. Additional Resources

- Forescout AMNESIA:33 Webpage - https://www.forescout.com/research-labs/amnesia33/
- CISA ICS Advisory ICSA-20-343-01 - https://us-cert.cisa.gov/ics/advisories/icsa-20-343-01
- Spacelabs Patch Qualification Customer Portal - https://www.spacelabshealthcare.com/products/security/patch-test-reports-access-form/?redirect_to=%2Fproducts%2Fsecurity%2Fpatch-test-reports%2F

5. Document History

Version	Release Date	Purpose
Rev A	December 15, 2020	AMNESIA:33 Vulnerability Assessment and Potential Product Impact Statement

6. 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.