SPACELABS HEALTHCARE

Security Advisory

"Name:Wreck" Vulnerability Assessment and Potential Product Impact Statement

Ref Doc ID	Version	Release Date	Advisory Status	Related CVE(s)
079-0272-00	A	<2024-07-26>	ACTIVE	CVE-2016-20009

1. VULNERABILITY OVERVIEW

Spacelabs Healthcare has been made aware of "Name:Wreck" vulnerabilities that affect Domain Name System (DNS) implementations. The "Name:Wreck" vulnerabilities refers to a set of nine DNS-related vulnerabilities found in four widely used open-source TCP/IP stacks: FreeBSD, IPNet, NetX, and Nucleus NET.

The potential impacts of these vulnerabilities include:
- DNS Cache Poisoning
- Denial of Service (DoS)
- Remote Code Execution (RCE)

These vulnerabilities arise from implementation issues within the TCP/IP stacks, often due to the complexities and misinterpretation of DNS standards.

2. RISK ASSESSMENT SUMMARY

Spacelabs has conducted an assessment to identify the potential impact on our products. Our assessment has found that one of the identified vulnerabilities impacts Spacelabs patient monitors (Qube, Qube Mini, and Xprezzon).

Spacelabs utilizes Wind River VxWorks IPNet identified as one of the TCP/IP stacks affected by the "Name:Wreck" for the patient monitors. The specific vulnerability in IPnet for VxWorks is identified as CVE-2016-20009, which affects the message compression feature.

Spacelabs has assessed the potential impact of this vulnerability on the Patient Monitors to be low. The vulnerability has been fixed on patient monitor SW v3.07 and later.

Customers with patient monitor Qube, Qube Mini, and Xprezzon running on patient monitor SW v3.07 or later are unaffected by this vulnerability.

3. RECOMMENDATIONS

Spacelabs recommends the following:

- Customers with Patient Monitors running on SW v3.06 or older should contact Spacelabs Technical Support to schedule the upgrades. See contacts below.
  - Customers in the United States may contact Technical Support to schedule their monitor 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 monitor 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 monitor SW upgrade to the current General Release version.
  - Phone: (+44) 1992 507 740
  - Email: emea.service@spacelabs.com

GENERAL SECURITY RECOMMENDATIONS

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

- Apply applicable upgrades to products when available and after validation.
- Minimize network exposure for all patient monitoring devices such as Monitors Qube, Qube Mini, and Xprezzon by network segmentation, placement of these devices behind hospital firewalls, and ensuring they are not accessible from the internet.
- Block suspicious external IP addresses at the hospital firewall. Monitor traffic internally for unusual behavior.
- Use secure methods such as Virtual Private Networks (VPNs) when remote access is required. VPNs may have vulnerabilities and should update to the most current version available. Also, be aware that a VPN is only as secure as its connected devices.
- Implement defense-in-depth within the enterprise environment with tools including Intrusion Detection/Prevention Systems (IDS/IPS), firewalls, and network access control (NAC).
- Implement and maintain an anti-malware solution and an endpoint detection 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-privileged basis.
- Have backup and restore processes and procedures established for disaster recovery and incident response.
- Monitor and maintain account provisioning and access control based on the principle of least privilege.

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 2016 Windows Server 2019	Not impacted

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	Not impacted
Xhibit 96102 / XC4 96501	Windows 10 IoT Enterprise	Not impacted
Bedside Monitors • Xprezzon 91393 • Qube 91390 • Qube Mini 91389	VxWorks 6.6	Impacted
DM3, DM4 Monitor	Windows 10	Not impacted

Diagnostic Cardiology (DC) Products

PRODUCT	OPERATING SYSTEM	IMPACT ASSESSMENT
Sentinel	Windows 10 Windows 11	Not impacted
Sentinel (server)	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 and 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

SPACELABS HEALTHCARE

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

5. Additional Resources

#	RESOURCE	URL
1	Wind River Support Network	https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2016-20009
2	National Vulnerability Database (NVD)	https://nvd.nist.gov/vuln/detail/CVE-2016-20009
3	CISA	https://www.cisa.gov/news-events/alerts/2021/04/15/namewreck-dns-vulnerabilities
4	Forescout	https://www.forescout.com/resources/namewreck-breaking-and-fixing-dns-implementations/

6. Document History

Version	Release Date	Purpose
Rev A	2024-07-26	“Name:Wreck” 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.

SPACELABS HEALTHCARE