SPACELABS
HEALTHCARE

Security Advisory

"PrintNightmare" Vulnerability Assessment and Potential Product Impact Statement

Ref Doc ID	Version	Release Date	Advisory Status	Related CVE(s)	Risk
079-0243-00	B	28 July 2021	ACTIVE	CVE-2021-34527	Moderate

1. VULNERABILITY

Spacelabs Healthcare has been made aware of a recently published vulnerability known as "PrintNightmare" (CVE-2021-34527) that exploits an underlying Windows service used for print services. Microsoft has issued guidance to address the vulnerability.

Per Microsoft, when the Windows Print Spooler service performs privileged file operations, a remote code execution can occur that can enable a threat to run arbitrary code with elevated SYSTEM privileges. This vulnerability affects all Windows operating systems and can include enterprise Domain Controllers. Exploitation of the vulnerability can enable an attacker to execute privileged commands on the target system.

Spacelabs has conducted an assessment to identify the potential impact to our products. Our assessment has found that Spacelabs products hosted on systems using Microsoft Windows operating systems can be impacted.

Some of the Spacelabs products use printing services as part of their clinical workflow, including ICS, Xhibit and Sentinel. Spacelabs embedded products that utilize Microsoft Windows Embedded OS are also impacted, including Xhibit, XC4 and Xhibit Telemetry Receiver (XTR).

For customer-hosted Spacelabs products, we recommend following Microsoft's recommendations to address the PrintNightmare vulnerability and advise applying the appropriate updates to remediate the vulnerability.

Spacelabs is working on a patched software release for Xhibit, XC4 and XTR that will incorporate the corrective patches from Microsoft.

2. RISK ASSESSMENT SUMMARY

Spacelabs considers the operational risk to its devices from a PrintNightmare attack to be Moderate.

In our review of the impact of this threat, due to the fact that a properly configured firewall in the hospital network would mitigate the likelihood of an attack from outside the organization, and since remote code execution would require that a bad actor already be positioned within the hospital network as a result of a prior attack, we have concluded that there is only a limited chance that a device could be compromised.

Security patches to remediate the vulnerability can found on Microsoft's website for most Microsoft's operating systems. Customers are encouraged to disable the Print Spooler Service if print services are not required, and to ensure that the hospital maintain a secure network firewall to protect its products and data.

3. RECOMMENDATIONS

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

- Apply the appropriate Windows updates to affected systems.
- If print services are not required, disable the Print Spooler service as instructed in Microsoft's guidance. This can be implemented on a system locally or via Group Policy.
- 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.
- Minimize network exposure for all patient monitoring devices such as Monitors and Patient Surveillance devices (Xhibit Central Station and Xhibit XC4) with the use of network segmentation, placement of these devices behind hospital firewalls and ensure that they are not accessible from the Internet. Additionally, do not expose Spacelabs product servers to the Internet when not required.
- 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.

4. EXAMINATION OF SPACELABS PRODUCTS

4.1 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.

SPACELABS HEALTHCARE

Patient Monitoring and Connectivity Products

Product	Host Operating System	Impact Assessment
XprezzNet 96190	Windows Server 2012 R2 Windows Server 2016	Impacted
Intesys Clinical Suite (ICS)	Windows Server 2012 R2 Windows Server 2016 Windows Server 2019	Impacted
Intesys Clinical Suite (ICS) Clinical Access Workstations	Windows 8.1 Windows 10	Impacted
Xhibit Telemetry Receiver (XTR) 96280	Windows Embedded Standard 7 SP1 Windows 10 IoT Enterprise Version 1809	Impacted
Xhibit 96102 / XC4 96501	Windows Embedded Standard 7 SP1 Windows 10 IoT Enterprise Version 1809	Impacted
Bedside Monitors • Xprezzon 91393 • Qube 91390 • Qube Mini 91389 • Ultraview SL 91367, 91369, 91370, and 91387	VxWorks 6.6	Not impacted

Diagnostic Cardiology Products

Product	Host Operating System	Impact Assessment
Sentinel	Windows 7 Windows 10 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019	Impacted
Pathfinder SL	Windows 7 Windows 10	Impacted
Lifescreen Pro	Windows 10	Impacted
Lifecard CF	No OS	Not impacted
EVO	No OS	Not impacted
Eclipse Pro	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

SPACELABS HEALTHCARE

Safe N Sound

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

5. Additional Resources

- Microsoft Security Response Center - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527
- Emergency Directive 21-04 Mitigate Windows Print Spooler Service Vulnerability - https://cyber.dhs.gov/ed/21-04/
- Spacelabs Patch Qualification Customer Portal - https://www.spacelabshealthcare.com/products/security/patch-test-reports-access-form/?redirect_to=%2Fproducts%2Fsecurity%2Fpatch-test-reports%2F

6. Document History

Version	Release Date	Purpose
Rev B		PrintNightmare 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.