SPACELABS HEALTHCARE

Security Advisory

SolarWinds Orion Code Compromise Threat Assessment and Potential Product Impact Statement

Ref Doc ID	Version	Release Date	Advisory Status	Related Security Directive	Operational Risk
079-0239-00	A	December 21, 2020	ACTIVE	CISA Emergency Directive 21-01 https://cyber.dhs.gov/ed/21-01/	Low

1. VULNERABILITY

Spacelabs Healthcare has been made aware of a vulnerability affecting SolarWinds Orion Platform software builds that could potentially allow an attacker to compromise the server(s) (creates a backdoor) on which the SolarWinds Orion products run. The U.S. government has issued an Emergency Directive to disconnect all devices which use SolarWinds Orion products within their environments. This is in response to news published last week and over the weekend that SolarWinds products were exploited and leveraged by nation-state actors to access sensitive systems in both private enterprises and the government; in other words, it was and by some accounts still is a supply-chain attack to gain access to sensitive target systems.

SolarWinds Inc. is an American company that develops software for businesses to help manage their networks, systems, and information technology infrastructure. SolarWinds Orion is a product platform that is used by enterprise IT departments and vendors to remotely manage and support networked devices. In general, these types of platforms are designed to access a wide gamut of devices and perform remote support and management — activities that typically require administrative privileges. Therefore, anyone who attains some level of administrative access to this platform would have the keys "backdoor" to the server/system.

CISA Emergency Directive: https://cyber.dhs.gov/ed/21-01/

2. RECOMMENDATIONS

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

- If the customer's IT department is running SolarWinds Orion, follow their company's security incident management and vulnerability management policies and procedures.
- 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.

3. EXAMINATION OF SPACELABS PRODUCTS

3.1 ASSESSMENT OF SPACELABS PRODUCTS

None of the Spacelabs product lines are impacted. While Spacelabs products do not use SolarWinds Orion, Spacelabs customers may be using SolarWinds Orion to manage and monitor their IT infrastructure. This infrastructure could include Intesys Clinical Suite (also known as ICS or Clinical Access) workstations or any Spacelabs product servers in their environment.

In response to the latest SolarWinds vulnerability, Spacelabs has conducted an assessment to identify devices potentially at risk for this SolarWinds Orion Code Compromise. 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	XprezzNet has no dependency on SolarWinds Orion. However, the customer IT department may use SolarWinds Orion to manage and monitor the server. We recommend that the use of the vulnerable SolarWinds Orion be discontinued.
Intesys Clinical Suite (ICS)	Windows Server 2012 R2, Windows Server 2016	ICS has no dependency on SolarWinds Orion. However, the customer IT department may use SolarWinds Orion to manage and monitor the server. We recommend that the use of the vulnerable SolarWinds Orion be discontinued.

Xhibit Telemetry Receiver (XTR) 96280	Windows Embedded Standard 7 SP1	No Impact
Xhibit 96102 / XC4 96501	Windows Embedded Standard 7 SP1	No Impact
Bedside Monitors • Xprezzon 91393 • Qube 91390 • Ultraview SL	VxWorks 6.6	No Impact

Diagnostic Cardiology Products

Product	Host Operating System	Impact Assessment
Sentinel	Windows 7 & 10, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019	Sentinel has no dependency on SolarWinds Orion. However, the customer IT department may use SolarWinds Orion to manage and monitor the server. We recommend that the use of the vulnerable SolarWinds Orion be discontinued.
Pathfinder SL	Windows 7, Windows 10	Pathfinder SL has no dependency on SolarWinds Orion. However, the customer IT department may use SolarWinds Orion to manage and monitor the server. We recommend that the use of the vulnerable SolarWinds Orion be discontinued.
Lifecard CF	No OS	No Impact
EVO	No OS	No Impact
CardioExpress SL6A SL12A / CardioExpress SL18A	Embedded OS	No Impact
ABP • OnTrak • 90217A • 90207	No OS	No Impact

Safe N Sound

Product	Host Operating System	Impact Assessment
Spacelabs Cloud	Varies	No impact
SafeNSound	Not applicable	No impact

4. Additional Resources

- Spacelabs Cybersecurity Information – https://www.spacelabshealthcare.com/products/security/
- Spacelabs Security Advisories - https://www.spacelabshealthcare.com/products/security/security-advisories-and-archives/
- Spacelabs Patch Qualification Customer Portal - https://www.spacelabshealthcare.com/products/security/patch-test-reports-access-form/?redirect_to=%2Fproducts%2Fsecurity%2Fpatch-test-reports%2F
- US Government DHS Emergency Directive - https://cyber.dhs.gov/ed/21-01/
- SolarWinds Security Advisory - https://www.solarwinds.com/securityadvisory
- Microsoft Advisory – https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/
- CISA Statement – https://us-cert.cisa.gov/ncas/current-activity/2020/12/13/active-exploitation-solarwinds-software

5. Document History

Version	Release Date	Purpose
Rev A	December 21, 2020	SolarWinds Orion Code Compromise Threat 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.