Security Advisory

Artifex Ghostscript Vulnerability Assessment and Potential Product Impact Statement

Ref Doc ID	Version	Release Date	Advisory Status	Related CVE(s)
079-0241-00	A	21 August 2023	ACTIVE	CVE-2023-36664

1. VULNERABILITY OVERVIEW

Spacelabs Healthcare has been made aware of a recently published security vulnerability within Artifex Ghostscript versions earlier than 10.02.1. This flaw occurs due to a mishandled permission validation for pipe devices (with the %pipe% prefix or the | pipe character prefix. It was discovered that Ghostscript does not properly handle permission validation for pipe devices, which could result in the execution of arbitrary commands if malformed document files are processed.

2. RISK ASSESSMENT SUMMARY

Spacelabs has conducted an assessment to identify the potential impact of Artifex Ghostscript vulnerability on our products. Our assessment has found that Spacelabs Sentinel Model 98200 & 98201 are affected by this vulnerability.

Spacelabs Sentinel Cardiology Information Management System incorporates a third-party application called Docuprinter LT. This application in turn relies upon Ghostscript.

Spacelabs has assessed the potential impact of this vulnerability on the Sentinel product. We have concluded that due to the way Docuprinter (Ghostscript) is used within Sentinel then this vulnerability does not result in an increased risk.

This is based on our understanding of the vulnerability and that it relies upon the ability to pass a specially crafted file into Ghostscript. Sentinel does not make use of, and/or expose this functionality. Docuprinter LT is only used as a virtual printer driver to generate a PDF file based on information generated internally within Sentinel.

The presence of Ghostscript on a system, independent of its use by Sentinel, may have slight impact on the overall risk. However, given that the vulnerability does not result in an elevation of privileges and an exploit would require access to the system this is considered small.

As Spacelabs continue to gain a deeper understanding of the impact of this vulnerability, we will continue to publish technical information to help customers detect, investigate, and mitigate the vulnerability across all our products where applicable.

3. RECOMMENDATIONS

3.1 WORK AROUNDS AND MITIGATIONS FOR SENTINEL

If the customer does not use the Cardio Direct Stress (CDStress) Functionality of Sentinel:

In this case, you can uninstall Docuprinter LT that includes Ghostscript from the system.

To uninstall Docuprinter, follow the below steps:

1. Search for "Add or Remove Programs" and Click on the first result.
2. In Apps and Features window, search for "Docuprinter".
3. Select "Docuprinter" and click on "Uninstall".

If the customer does use Cardio Direct Stress (CDStress) Functionality of Sentinel:

Docuprinter is required to support CDStress so cannot be uninstalled if this feature is being used. Please ensure you are following all the security recommendations in section 3.2.

3.2 GENERAL SECURITY RECOMMENDATIONS

- Monitor and maintain account provisioning and access control based on the principle of least privilege.
- Enable multi-factor authentication where possible.
- Block suspicious external IP addresses at the enterprise firewalls. Monitor traffic internally for unusual behavior.
- Implement defense-in-depth within the enterprise environment consisting of tools such as intrusion detection systems/intrusion 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.
- Apply applicable patches, hotfixes, and updates to servers and products when available and after they have been validated.

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	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 Windows Server 2019	Not impacted.

Intesys Clinical Suite (ICS) Clinical Access Workstations	Windows 10	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.

Diagnostic Cardiology (DC) Products

Product	Host Operating System	Impact Assessment
Sentinel	Windows 10 Windows 11 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019	Impacted.
Pathfinder SL	Windows 10	Not impacted.
Lifescreen Pro	Windows 10 Windows 10	Not impacted.
Lifecard CF	No OS	Not impacted.
EVO	No OS	Not impacted.
Eclipse Pro	No OS	Not impacted.
ABP • OnTrak • 90217A • 90207	No OS	Not impacted.

SafeNSound (SNS)

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

Rothman Index (RI)

Product	Host Operating System	Impact Assessment
RI Cloud	Varies	Not impacted.
Rothman Index	Not applicable	Not impacted.

5. Additional Resources

#	Resource	URL
1	CVE-2023-36664 Detail	https://nvd.nist.gov/vuln/detail/CVE-2023-36664
2	Proof of Concept Developed for Ghostscript CVE-2023-36664 Code Execution Vulnerability	Ghostscript Remote Code Execution Vulnerability | Kroll
3	Ghostscript Overview	Ghostscript

6. Document History

Version	Release Date	Purpose
Rev A	21 Aug 2023	Artifex Ghostscript 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.