Security Advisory

Mirth Connect RCE Vulnerability Assessment and Potential Product Impact Statement

Ref Doc ID	Version	Release Date	Advisory Status	Related CVE(s)
079-0268-00	A	2023-11-07	ACTIVE	CVE-2023-43208 CVE-2023-37679

1. VULNERABILITY OVERVIEW

Spacelabs Healthcare has been made aware of a third-party issue with the NextGen Healthcare Mirth Connect Remote Code Execution (RCE) vulnerability named CVE-2023-43208.

Mirth Connect is **not** a Spacelabs product but may be used by customers to manage connectivity across various products/platforms.

Mirth Connect, before version 4.4.1, is vulnerable to an unauthenticated remote code execution. Note that this vulnerability is caused by the incomplete patch that was issued for CVE-2023-37679.

2. RISK ASSESSMENT SUMMARY

Spacelabs has conducted an assessment to identify the potential impact of the Mirth Connect Remote Code Execution (RCE) vulnerability on our products. Our assessment has found that Spacelabs products such as Intesys Clinical Suite (ICS), XprezzNet, SafeNSound, Sentinel and Rothman Index that are configured to leverage Mirth Connect are affected by this vulnerability.

Mirth Connect, by NextGen HealthCare, is a third-party open-source data integration platform interface engine used in the healthcare industry to communicate and exchange data between disparate systems in a standard format.

This is an unauthenticated remote code execution vulnerability which would most likely be exploited for initial access or to compromise sensitive healthcare data. Traffic sent by Spacelabs systems such as Intesys Clinical Suite (ICS), XprezzNet, SafeNSound, Sentinel and Rothman Index may be compromised by malicious attackers as the data passes through Mirth Connect version that is affected by this vulnerability.

Spacelabs has assessed the potential impact of this vulnerability to be low on Intesys Clinical Suite (ICS), XprezzNet, SafeNSound, Sentinel and Rothman Index products, since the vulnerability exists on the third-party application Mirth Connect. The primary security concern is in the data exchange though the Mirth Connect where healthcare data can be exposed.

As Spacelabs continues 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

- US customers may reach out to Technical Support to schedule their Mirth Connect upgrade to version 4.4.1 or later.
  - Phone: (+1) 800-522-7025
  - Email: support@spacelabs.com

- Canada customers may reach out to Canada Technical Support to schedule their Mirth Connect upgrade to version 4.4.1 or later.
  - Phone: (+1) 905 564 2229
  - Email: SLCanadaCustomerService@spacelabs.com

- International customers may reach out to Global Technical Support to schedule their Mirth Connect upgrade to version 4.4.1 or later.
  - Phone: (+44) 1992 507 740
  - Email: GTSDC@spacelabs.com

GENERAL SECURITY RECOMMENDATIONS

- Both CVE-2023-43208 and previous CVE-2023-37679 indicate the Mirth Connect (web) management interface to be the point of exploitation – restrict traffic (IP addresses) to his web interface except for trusted sources.
- 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.
- 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.
- Monitor and maintain account provisioning and access control based on the principle of least privilege.
- Enable multi-factor authentication where possible.

- 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	OPERATING SYSTEM	IMPACT ASSESSMENT
XprezzNet 96190	Windows Server 2012 R2 Windows Server 2016 Windows Server 2019	Impacted (if connected to Mirth)
Intesys Clinical Suite (ICS)	Windows Server 2012 R2 Windows Server 2016 Windows Server 2019	Impacted (if connected to Mirth)
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 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
DM3, DM4 Monitor	Windows CE Windows 10	Not impacted

Diagnostic Cardiology (DC) Products

PRODUCT	OPERATING SYSTEM	IMPACT ASSESSMENT
Sentinel	Windows 10 Windows 11	Not impacted
Sentinel (server)	Windows Server 2012 R2 Windows Server 2016 Windows Server 2019	Impacted (if connected to Mirth)
Pathfinder SL	Windows 10	Not impacted
Lifescreen Pro	Windows 10	Not impacted
Lifecard CF	No OS	Not impacted

PRODUCT	OPERATING SYSTEM	IMPACT ASSESSMENT
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

SafeNSound (SNS)

PRODUCT	OPERATING SYSTEM	IMPACT ASSESSMENT
Spacelabs Cloud	Varies	Not impacted
SafeNSound	Not applicable	Impacted (if connected to Mirth)
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	Impacted (if connected to Mirth)
Rothman Index mobile		Not Impacted

5. Additional Resources

#	RESOURCE	URL
1	CVE-2023-43208 Detail	https://nvd.nist.gov/vuln/detail/CVE-2023-43208
2	Securityweek article	https://www.securityweek.com/critical-mirth-connect-vulnerability-could-expose-sensitive-healthcare-data/
3	Horizon3.ai (Security firm) article	NextGen Mirth Connect Remote Code Execution Vulnerability (CVE-2023-43208) – Horizon3.ai
4	Hackernews article	https://thehackernews.com/2023/10/critical-flaw-in-nextgens-mirth-connect.html

#	RESOURCE	URL
5	CVE-2023-37679 Detail	https://nvd.nist.gov/vuln/detail/CVE-2023-37679

6. Document History

Version	Release Date	Purpose
Rev A	11-07-2023	Vulnerability Assessment and Potential Product Impact Statement-Mirth Connect RCE-Vulnerability

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.