MX-9274 - Getinge Product Security Advisory PSA-2024-DEC Maquet Critical Care MSync

Publication Date

2024-12-16 Gothenburg, Sweden

Overview

Getinge, as a leading medical device manufacturer, is committed to ensuring medical device cybersecurity for our customers. As part of this engagement, Getinge continuously identifies, analyses, and addresses potential vulnerabilities in our products, often in collaboration with customers and researchers. In accordance with Getinge's Coordinated Vulnerability Disclosure process, the company is proactively issuing an advisory regarding the MSync product line.

Getinge internal review has revealed that The serial protocol to HL7 conversion product MSync has been found to contain a set of software vulnerabilities CVE-2023-43208 and CVE-2023-37679 that are part of the Mirth Connect SW library utilized in MSyncs HL7 protocol conversion.

Exploitability

To exploit the vulnerabilities, it is necessary to have access to a local hospital network with devices that actively use MSync to convert data to HL7 and send it over the network. All versions of MSync are affected but only in the HL7 conversion configuration. The configuration used to support Cardiohelp with USB to RS232 conversion is not affected.

Potentials hazards

Potential hazards include the possibility to tamper with the device function of converting data to HL7 format or allow exploitation of the device as a steppingstone for infiltration of the connected network.
No patient risk is considered to be associated with the issue, since MSync does not perform patient treatment and does not affect point of care device usage.

At this time Getinge is not aware of any indications of the vulnerabilities having been exploited. If you suspect that your MSync system has been tampered with or otherwise been exposed to potential hazards described in this letter, please report it via Security (getinge.com) or contact your local Getinge representative.

Affected Products

Product Article number:

MSync: 68 81 603, All system SW versions

Recommendations

- Getinge recommends our customers to perform their own risk analysis and if needed stop the usage of MSync by disconnecting the product from the network.
- Stop using the device and contact your local sales representative if you believe that your device has been compromised.

Legal Notice

This Product Security Advisory is based on all our findings at the time of publication. As more information becomes available, it is possible that it may result in changed assessments or that assessments contained in this advisory may turn out to be incorrect. We also reserve the right to change or revoke any recommendations. However, additional factors may be present due to individual circumstances on-site. As this information is unavailable to Getinge, Getinge can therefore not guarantee that the information presented here is conclusive. Please check carefully to what extent deviations can arise for a specific individual case. If necessary, you will be informed about new findings through a subsequent Getinge Product Security Advisory.

Revision History

Rev.	Date	Description
1	2024-12-16	Initial version