MX-9245 - Getinge Product Security Advisory PSA-2024-OCT Maquet Critical Care Flow-i_c_e

1 LEGAL NOTICE

This Product Security Advisory is based on all our findings that we had at the time of publication. However, the facts of the case are being reviewed on an ongoing basis and it is possible that this 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. In addition, differences may result from the circumstances of the individual case on site. This information is naturally not available to us and has not been taken into account. Getinge can therefore accept no responsibility that the information presented here is conclusive or comprehensively correct for you. Therefore, please check carefully to what extent deviations can arise for your individual case. If necessary, you will be informed about new findings through following advisories

2 PUBLICATION DATE

October 23, 2024
Gotheburg, Sweden

3 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 Flow-i/c/e product lines.

Getinge internal tests have revealed a cybersecurity related misconfiguration in Flow-i/c/e software when used in connecting the devices to Connected Services. Connected Services is part of a service plan offered by Getinge to enable hospitals to access digital equipment data. The service is provided either through a direct wired connection to Getinge servers or via the Getinge Connect module (X10/X20 models).

4 EXPLOITABILITY

To exploit the vulnerability, it is necessary to have access to a local hospital network with devices that actively use Connected Services without the Getinge Connect module (X10/X20). The vulnerability can only be exploited for a few seconds during start-up or when the device is connected for sending logs. By design this cannot

occur during patient treatment, but non-temporary changes to configuration cannot be ruled out.

5 POTENTIALS HAZARDS

Potential hazards are possibility to tamper with non-English language files and potentially or causing misleading information on the screen or the need to change anesthesia machines during the case. Additionally, remote code execution resulting in panel restarts during standby or treatment may be possible.
At this time Getinge is not aware of any indications of the vulnerability having been exploited. If you suspect that your anesthesia system has been tampered with or otherwise been exposed to potential hazards described in this letter, please report it via www.getinge.com/int/security or contact your local Getinge representative.

6 AFFECTED PRODUCTS AND SOLUTIONS.

Affected Products and solutions	Remediation
Flow-i: 6677200, 6677300, 6677400, 6888520, 6888530, 6888540 Flow-c: 6887700 Flow-e: 6887900 Flow System software versions 4.8.4 and 4.10	• If your Flow Family Anesthesia system is connected to Connected Services via a Getinge Connect module (X10/X20), no action is required. • If your Flow Family Anesthesia system is connected to Connected Services directly via the Ethernet port on the Flow Family Anesthesia system: Please contact your local Getinge representative to activate Connected Services with a Getinge Connect module. • Continued use of the Connected Services connection without a Getinge Connect module (X10/X20) is not recommended. • Stop using the device and contact your local sales representative if you have reason to believe that your device has been compromised. • Remediation is also described to customers in FSCA(Field Safety Notice) MX-9036

7 REVISION HISTORY

Rev.	Date	Description
1	23-Oct-2024	Initial version