Getinge Product Security Advisory
PSA-2023-MAR

"Pulsion PulsioFlex (PC4000)" and "Pulsion PiCCO2 (PC8500)"

Publication Date

30 June 2023
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 Pulsioflex (PC4000) and PiCCO2 (PC8500).

Through a cybersecurity audit made by Neodyme AG on a discontinued version of Pulsioflex (PC4000), Getinge was made aware of several vulnerabilities connected with the Windows XP operating system. The affected devices have remotely exploitable vulnerabilities like CVE-2017-0114. Others could be exploited by an attacker with physical access to the device.

Both PiCCO2 and PulsioFlex patient monitoring systems (with listed SW versions) run on the Windows XP Embedded operating system. Getinge used the technology that was current when the products were placed on the market. However, technological advancements (e.g. OS) and the lack of continuity by software manufacturers have affected support for older software versions. Due to the age of the affected devices, they cannot be upgraded to a newer OS and as of 2014 Microsoft has discontinued support for Windows XP. Therefore, no patches are available to fix the vulnerabilities

No significant increase in health risk has been linked to the vulnerabilities due to Pulsioflex intended use as a secondary monitor and limited use of its network connectivity (printing only). There are no indications from complaints or customer feedback that the vulnerabilities have been exploited in any kind of cyberattack.

Affected Products

Pulsion PulsioFlex PC4000 (manufacturing date before 2016)
SW versions: 1.0.0.3 A, 1.0.0.3 B, 2.1.0.3 A, 3.0.0.14 B, 3.0.0.14 US B, 3.1.0.10 B, 4.0.0.7 A, 4.0.0.11 US A, 5.0.0.15 A

Pulsion PulsioFlex PC4000 (manufacturing date after 2016)
SW versions: 3.0.1.3A, 5.0.1.1A

Pulsion PiCCO2 PC8500
SW versions: all versions

Recommendations

- Apply the methods described in IEC 80001-1:2021 to determine the risk of integrating PiCCO2 / PulsioFlex monitoring devices into your hospital IT infrastructure.
- The affected devices only require Ethernet connection for printing patient data reports. Consider not to connect the devices to hospital IT network via LAN if you are not using this functionality.
- Protect the used part of the hospital IT network from unauthorized access and structure it in such a way that an outside attacker cannot gain access to the monitoring devices by means of network segmentation or segregation.
- Prevent unauthorized (physical) access to the devices.
- Consider closing or applying physical locks to all unused USB ports.
- Stop using the device and contact your local sales representative if you believe that your device has been compromised or the warranty seal at the bottom of the device is missing / broken (see picture in Appendix, label [4]).

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. On the other hand, additional factors may be present from individual circumstances of the case on-site. As this information is not available to us and it may not be 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 specific individual case. If necessary, you will be informed about new findings through a subsequent Getinge Product Security Advisory.

References

Name	Link
IEC 80001-1:2021	Application of risk management for IT-networks incorporating medical devices — Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software

Revision History

Rev.	Date	Description
1	02-June-2023	Initial version

Appendix: How to identify affected products (Pulsion PulsioFlex only)

A Windows sticker (label [1]) is placed on the device bottom indicating the installed operating system:

- Grey sticker refers to Windows XP as an operating system
- Yellow sticker refers to Windows 7 as an operating system

From software version 5.1.1 Windows 7 as an operating system is installed. Newer PulsioFlex devices (PC4000) can be updated to such a version. The update to this software version is possible for monitors manufactured in 2016 (see label [2]) or later. The serial number (label [3]) needs to start with a 16 as the two first figures indicate the manufacturing year.