October 30, 2019

Re: **Cybersecurity Communication - Urgent/11 and Network Interface Unit (NIU) Users**

Dear Valued NIU Customer:

On October 1, 2019, the U.S. Food and Drug Administration ("FDA") issued a Safety Communication advising patients, health care providers, facility staff, and manufacturers about cybersecurity vulnerabilities that may introduce risks for certain medical devices and hospital networks.[1] In the communication, the FDA announced that security researchers identified eleven (11) cybersecurity vulnerabilities, (referred to as "Urgent/11"), and asked manufacturers to work with health care providers to identify medical devices that may be susceptible to the vulnerabilities. This letter is being sent pursuant to FDA's recommendation.

The Urgent/11 vulnerabilities exist within components of IPnet. IPnet has been incorporated into some versions of popular operating systems that are used in medical devices and hospital systems, including VxWorks (by Wind River) and other operating systems. The security researchers who identified Urgent/11 classified six (6) of the eleven (11) vulnerabilities as "critical". Hackers can exploit these vulnerabilities and take control of the medical device or impair function(s) of that device. Additionally, these vulnerabilities may allow hackers to install programs; view, change, or delete data; or create new accounts with full user rights. Only medical devices and hospital systems using or supported by an operating system that incorporated IPnet are susceptible to Urgent /11.

Hill-Rom is committed to networked medical device cybersecurity and risk mitigation in the design of its products. Based on the FDA communication on Urgent/11 we recently identified two products – the Network Interface Unit ("NIU") and version 1 of the Wireless Interface Unit ("WIU1") – that are susceptible to potential cybersecurity attacks, targeting the eleven (11) vulnerabilities, known as Urgent/11. No customers are currently using WIU1.

Following a risk assessment, Hill-Rom determined NIU cannot be hacked from outside of your network (*i.e.*, your network has to be hacked before the attack can control or prevent functions of NIU). There is no patch designed for NIU that would further mitigate the Urgent/11 vulnerabilities. To mitigate the cybersecurity vulnerabilities, we recommend you configure your network Intrusion Detection and Protection ("IDP") systems or Firewall per the guidelines from Armis, Inc. – the security firm that discovered Urgent/11. These guidelines, titled Urgent/11: Critical Vulnerabilities to Remotely Compromise VxWorks, the Most

[1] U.S. Food & Drug Administration, URGENT/11 Cybersecurity Vulnerabilities in a Widely-Used Third-Party Software Component May Introduce Risks During Use of Certain Medical Devices: FDA Safety Communication (October 1, 2019), https://www.fda.gov/medical-devices/safety-communications/urgent11-cybersecurity-vulnerabilities-widely-used-third-party-software-component-may-introduce.

Popular RTOS, can be found at https://go.armis.com/urgent11. While Hill-Rom takes protecting the safety and security of our products very seriously, cybersecurity protection is dependent on our customers' implementation of overall cybersecurity strategies and best practices that help safeguard their information and systems from threats. Cybersecurity is everyone's responsibility.

Hill-Rom continues to monitor for cybersecurity developments and their potential impact on our products. We will update you, our valued customer, of any relevant information.

If you have any questions, please contact us at 1-800-445-3730 Option 3, Option 1.

Sincerely,

Soundharya Nagasubramanian

Soundharya Nagasubramanian
Director, R&D, Product Information Security
Hill-Rom